Surveillance & Society
4(1/2): 136-153
http://www.surveillance-and-society.org

Report. Sub-lethal vision: varieties of military surveillance technology.

Steve Wright[1]

Introduction

The military have always used surveillance devices of one form or another. What characterises their procurement today is the wide variety of purposes to which they are deployed and the move towards semi-intelligent systems. The events of 9/11 and the so called revolution in military affairs (RMA) have merely accelerated an ongoing trend to build cybernetic military systems where weapons are simply the muscle deployed by a nervous system based upon an intelligent handling of data through communication, command and control (C3I).

However, the advent of nanotechnologies will inevitably change the way that such weapons and data are put together to achieve more effective target acquisition and destruction. Super miniaturization will enable individual soldiers to become part of a more efficient battlefield where commanders use surveillance to actually see through the helmets of their men. Individual tagging will identify friend from foe and prevent friendly fire but increasingly, surveillance technology will change the nature of targets as information dependent societies are hit by electrons rather than hot metal.

Indeed, ‘information warfare’ is part of a variety of new forms of emergent attack strategies. Most modern states are dependent on telecommunications infrastructure and many within military circles are asking why destroy civilian infrastructure if a country's nervous systems can be disabled instead. According to General Fogleman US Air Force Chief of Staff, ‘Dominating the information spectrum is as critical to conflict now as occupying the land or controlling the air has been in the past.’

Modern surveillance technology is becoming part of that infrastructure. Weapons now have in built primitive surveillance algorithms but supposedly neutral telecommunications infrastructure such as the mobile phone network can be used not only for surveillance but for pinpointing and targeting specific individuals and groups. Since weapons work on a digital target plan then digital items carried by most of us such as phones or ID smart cards can be used to programme target selection by other weapons.

[1] Praxis Centre, Leeds Metropolitan University. mailto:S.T.Wright@leedsmet.ac.uk

Another complicating factor is actually separating out which elements of a weapon system are actually surveillance mechanisms. So many weapons now are vast arrays of components with no one manufacturer or even country being responsible for the manufacture of the whole weapon. For example the Head up Displays used in US F16's Fighter Aircraft are manufactured in the UK[2] and then exported to America and subsequently used by Israelis to target Palestinians but are treated as non-lethal components in terms of export regulations.[3]

A preliminary goal for this report was to explore how the Revolution in Military Affairs (RMA) is creating new technologies to both facilitate and to target surveillance infrastructure and how no hiding place military doctrines will begin to inhabit future urban living spaces as the dictates of a growing international crisis move away from just mass supervision to more prophylactic systems of targeting. The author is particularly interested in how some types of new border control technologies can incorporate punishment with surveillance systems to become victim activated networks. However, it quickly became apparent that any deep questioning of where new doctrines of urban warfare will take future military surveillance capabilities could quickly become quite abstract.

For example, a recent presentation from the College of Aerospace, Doctrine Research and Education in the US[4], for example, listed quantum computers; intelligent software; virtual reality; intelligent materials; directed energy weapons, lasers; biotechnology; human/computer interfaces; mind control; micro-technology; millimetre wave cameras and video insertion amongst its emergent technologies. Many of these technologies have a surveillance dimension whether for targeting, for directed control, or for feedback on effectiveness.

The author is especially interested in the military's use of surveillance technology for internal control, counter revolutionary and anti-terrorist operations. After all, many of the hi-tech night-vision surveillance cameras and flight stabilized helicopter mounted CCTV systems which are familiar today originated in US military operations in Vietnam and the subsequent transfer to US police. It would be quite a challenge to explore how such civilian systems had been readopted and ruggedized for military applications. Yet in many senses the variety of possible themes is potentially too vast: from mechanical roboflies[5] to act as military micro spies to global telecommunications surveillance operated by the NSA.[6] In the end it seemed necessary to ground the material in what was currently on the market or being evaluated for future deployment. With that goal in mind, a visit was arranged to the Force Protection and Evaluation Demonstration at US Marine Corps HQ.

[2] *Hansard* 16 April 2002

[3] See Oxfam, Amnesty International and IANSA, Lock, Stock and Barrel, Control Arms Campaign, February 2004. http://www.controlarms.org/documents/lock_stock_barrel.pdf

[4] William A Stanmeyer, Emerging Technologies IW-270, College of Aerospace, Doctrine Research & Education. See http://www.afrl.af.mil

[5] *Financial Times*, 'Mechanical 'roboflies' lend wings to defence' 22 November 2001, p15. See also http://www.newswise.com/articles/view/502903/

[6] See the STOA reports to the European Parliament: Steve Wright, *An Appraisal of the Technologies of Political Control* and Duncan Campbell, *Interception Capabilities 2000*.

Force Protection Equipment Demonstration

The Force Protection Equipment Demonstration is organised every two years by the U.S. Department of Defense, at the Marine Corps Air Facility in Quantico – more famous because of its connotation with the X Files TV series since the FBI have their shooting ranges here too. This was the fifth such event and it took place from 26-28 April 2005 being co-sponsored by the Joint Staff, the Department of Energy (DoE), the National Institute of Justice (NIJ) and the Technical Support Working Group (TSWG).

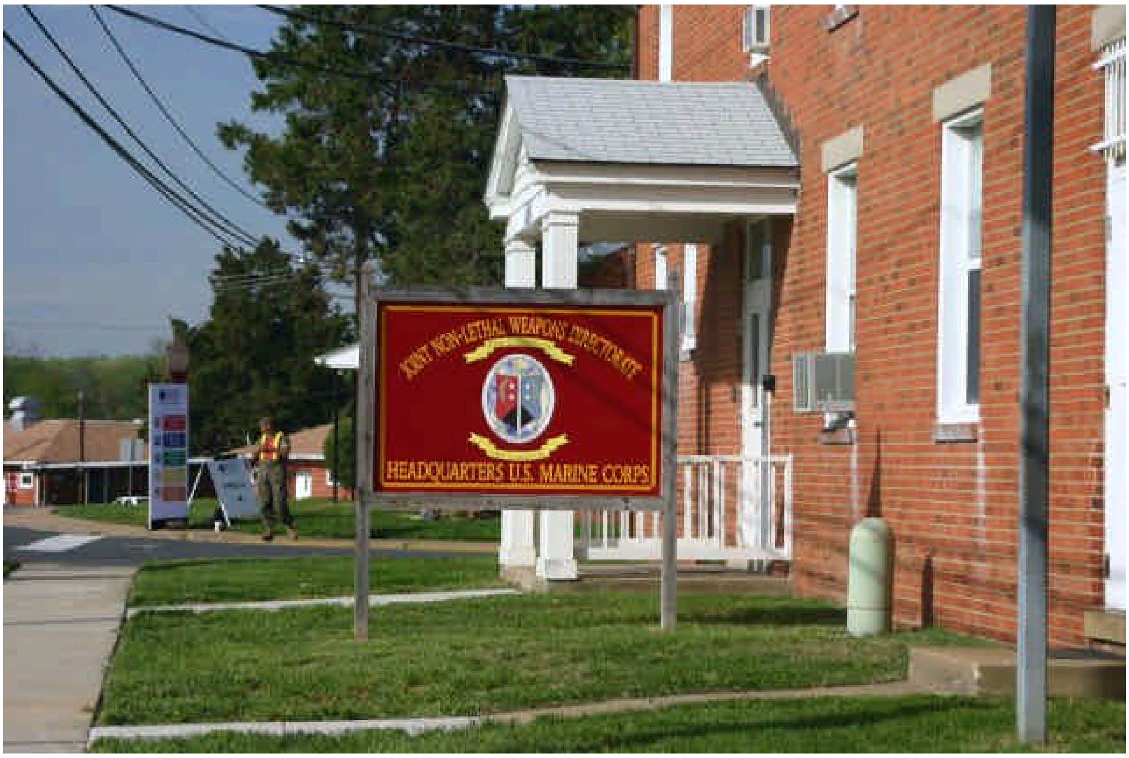
JOINT NON-LETHAL WEAPONS DIRECTORATE
HEADQUARTERS U.S. MARINE CORPS

Figure 1: Joint Non Lethal Weapons HQ

It was a strange feeling walking into the Marine Corp Base. Helicopters were landing and taking off continuously. I passed the HQ of the Joint Non-Lethal Weapons Directorate; another sign saying "MCNOSC – Shaping the Information Battle Space" and rather more disconcertingly given that my bag was full of cameras – a notice outside the expo site warning that it was a "Restricted Area: No Photography, No Admittance, No vehicles + Deadly Force Authorized…"

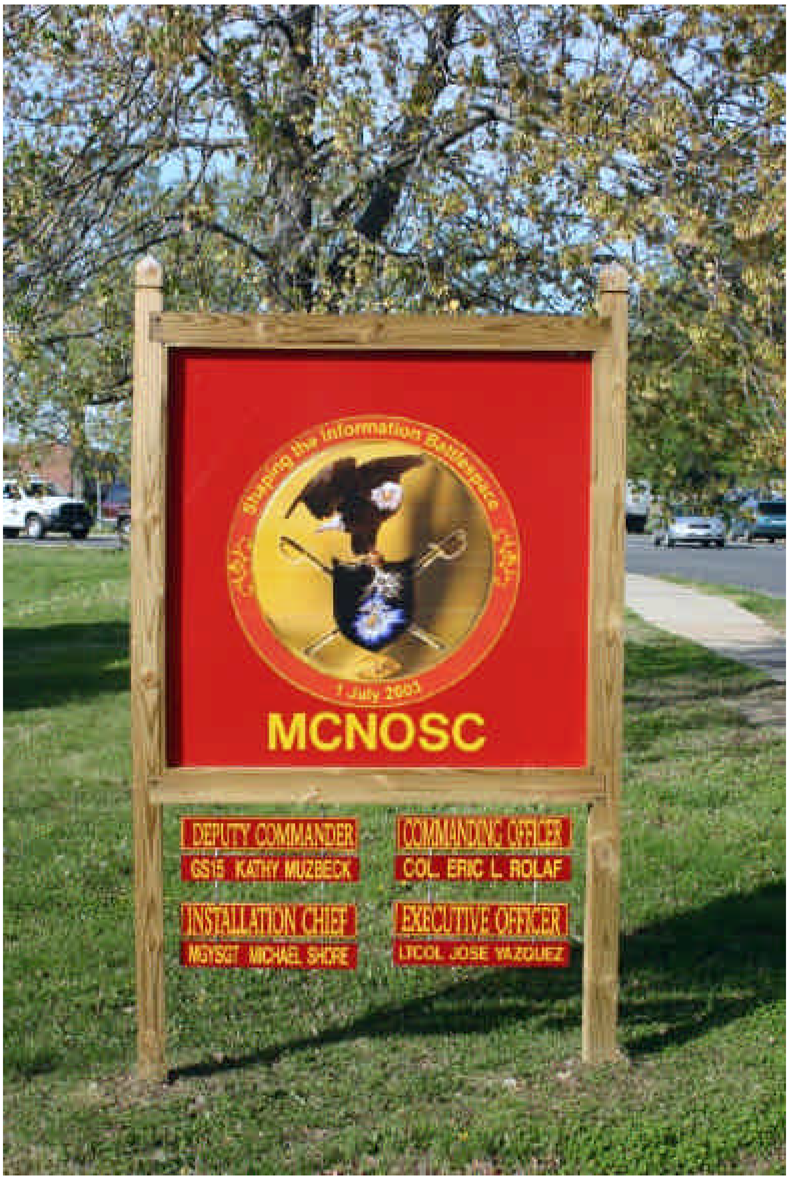

Figure 2: "Shaping the Information Battle Space"

FPED takes place adjacent to the vast airfield with two huge hangers offering more sheltered room to the more sensitive exhibits. All visitors were screened at entry and then subject to search by sniffer dogs before being bussed in. Huge queues built up since in term of access control, this was one the least efficient visitor entry processing approaches this author has experienced in the scores of security fairs that I have visited.

As a proving ground for state of the art security technologies, the event provided a realistic showcase for representative contemporary systems. These included automated entry control equipment, biometrics, blast/ballistics mitigation and protection, cargo inspection devices, communication equipment, delay and denial technologies, explosive ordnance disposal equipment, fence sensor equipment, robotics, night vision and optics, non-lethal technology, unattended ground sensors and physical security equipment. What awaited was a playground filled with futuristic surveillance toys – clearly, security in the 21st century is a very lucrative line of business.

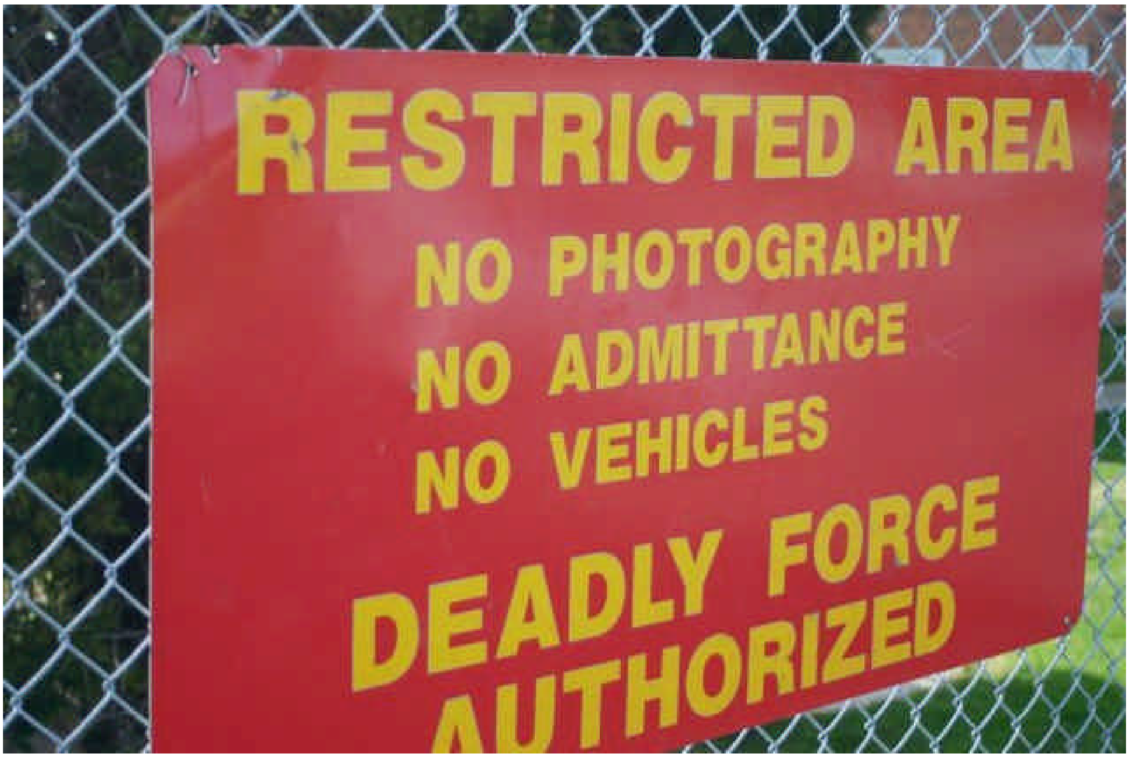

Figure 3: Lethal Advice for 'Non-Lethal' Arms Fair

Varieties of Military Surveillance

It is difficult to capture the entire range of surveillance on display since many of the systems incorporated sophisticated GIS or other computerised logic to enable real time tracking. However, it is worth describing just a few of the systems on display in further details in order to illustrate how surveillance capabilities are used to make other technologies more effective, efficient and precise in their given role. An ongoing role and function is to act as real-time feedback loop which can trigger other action or assess anomalies.

Intelligent Fencing

For example the fences on display had sensors to detect unauthorized entry. Some had electroshock stunning systems incorporated and were entirely victim activated. Other companies such as L3 Communications use a battlefield Anti-Intrusion System do ensure zone denial and detection.

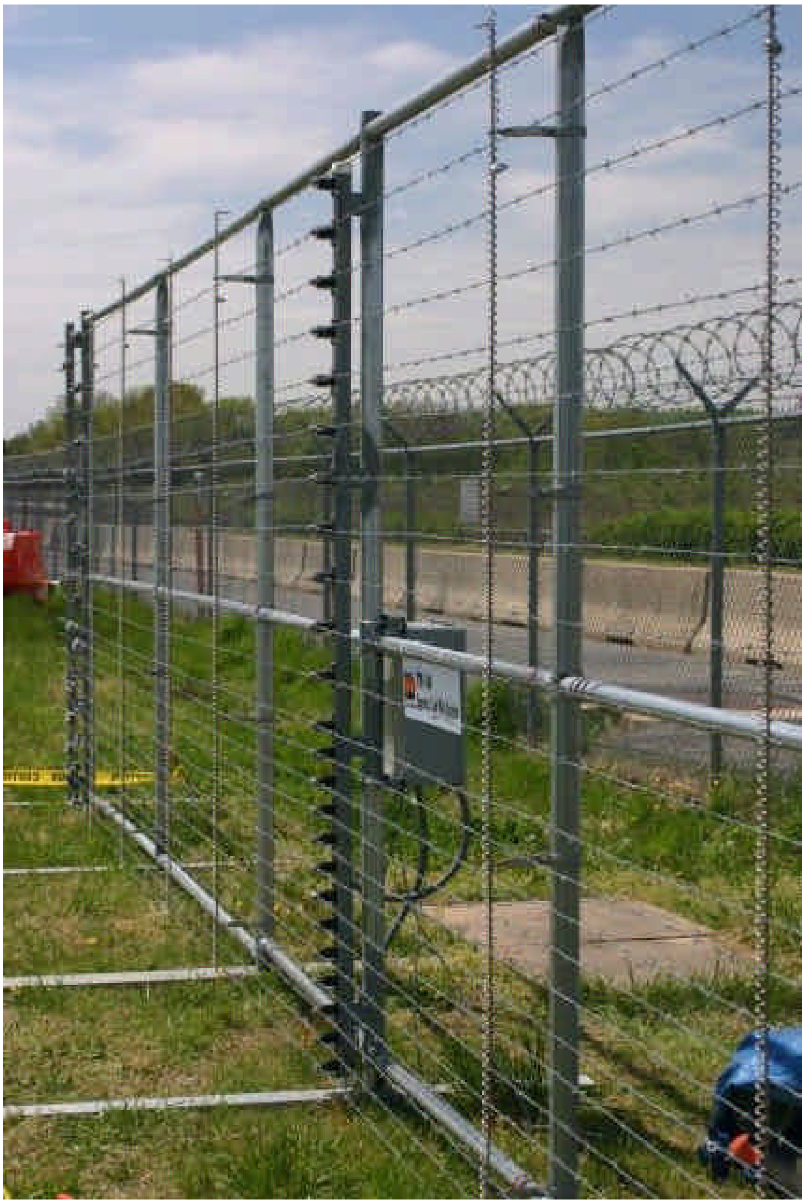

Figure 4: Electroshock Fencing

Remotely Operated Weapon Systems

Other perimeter control systems had more lethal facilities – for example the TRAP T-2500D by Precision Remotes, featured a sub-machine gun operated by remote control via an attached CCTV system. The USAF Security Forces Centre was also fielding a Common Remote Operating Weapons System (CROWS) with daytime CCTV, night vision, FLIR and laser range finder. Conversely, Israeli company Rafel have developed the Spotlite sniper detection system which uses electro-optic systems to accurately locate snipers day or night.

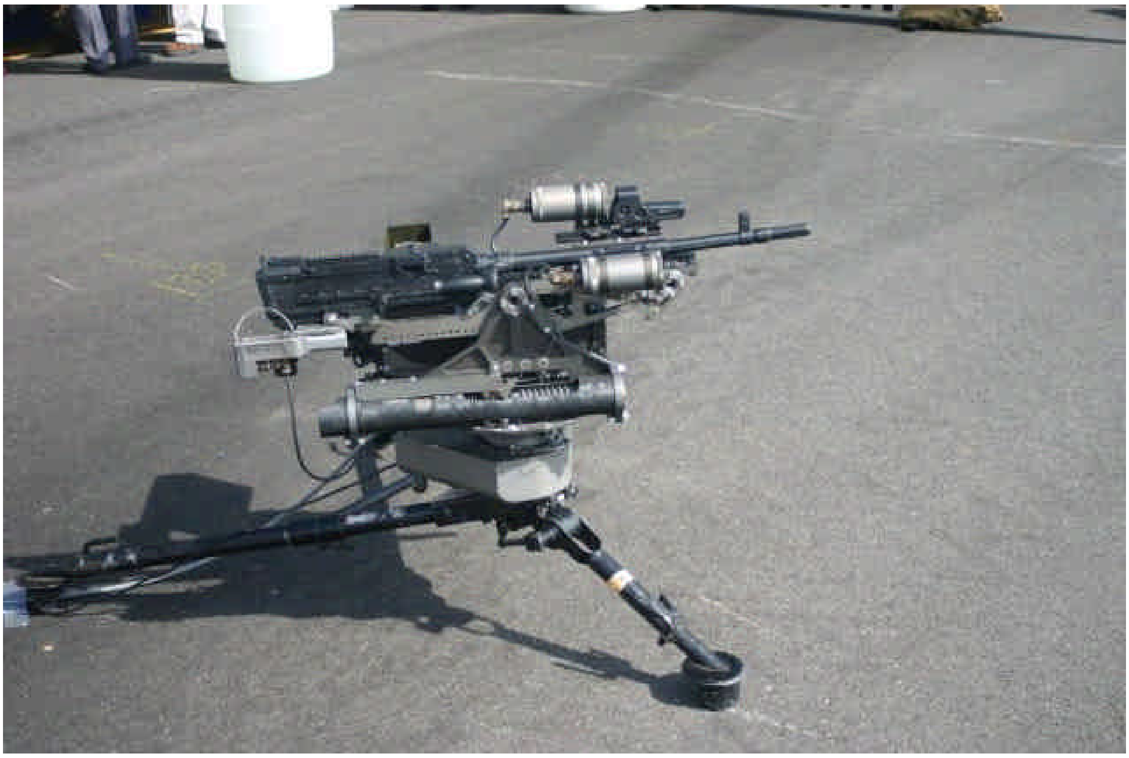

Figure 5: Precision Remote Machine Gun

Alternative Landmines

Several systems on display here used surveillance to create alternative anti personnel landmines. For example the Joint Non Lethal Weapons (JNLW) stand displayed a taser landmine which is a victim activated `weapon which projects several darts carrying 50,000 volts to immobilize someone for up to an hour. The JNLW) newsletter announced that the so called Taser Anti-Personnel Munition was successfully tested at the Picatinny Arsenal last October when it attacked moving targets up to a range of 21 feet using a Passive IR surveillance sensor rather than a trip wire.[7] (The newsletter didn't mention that in this configuration, the device would probably fall foul of the Ottawa anti-personnel landmines convention).

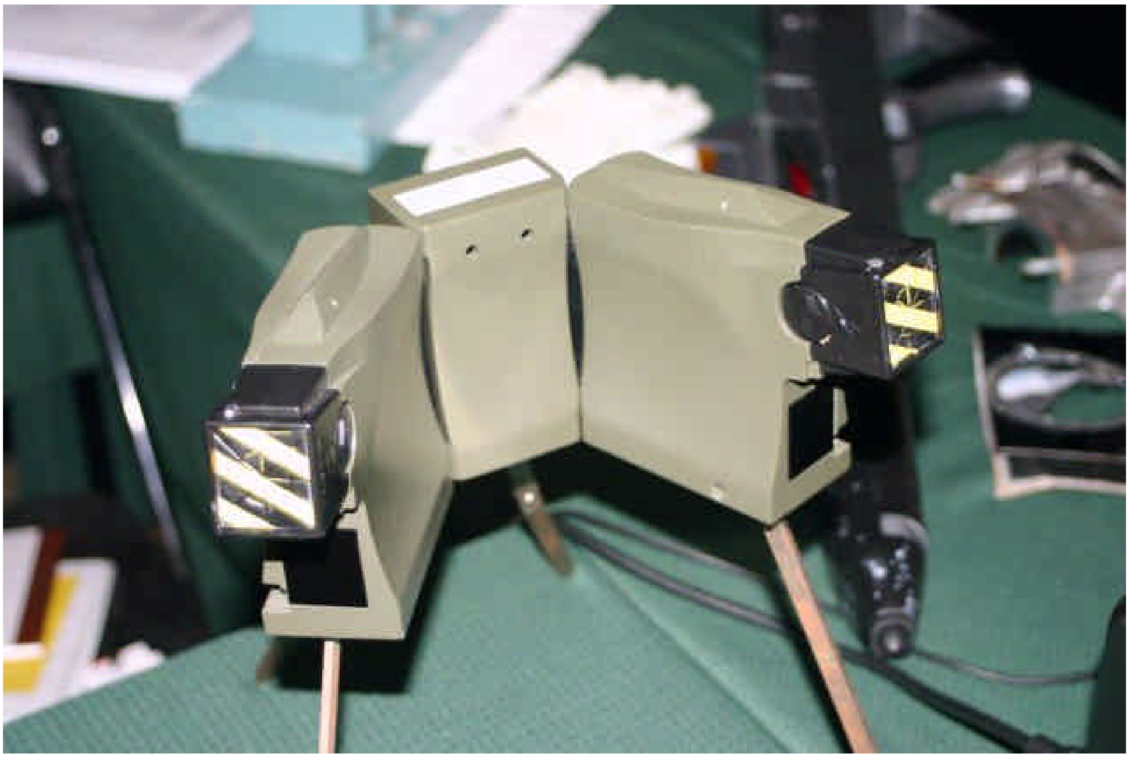

Figure 6: TASER Landmine

Another curiosity at this expo was the Metal Storm 40mm Prototype Weapon System which was a series of Mortars attached to a remotely operated Scout Vehicle., which was live demonstrated again at the Picatinny Arsenal in March 2005. Metal Storm started out as an Australian company which revolutionized guns by creating an electronic firing system capable of astonishing firepower of between 500,000 and a million rounds a minute. The company opened a North American subsidiary in the late Nineties after winning a three year $10.25 million grant from the US Defense Advanced Research projects Agency (DARPA). Art Schatz, a senior VP

[7] Joint Non-Lethal Weapons Directorate 'Safeguarding Peace –Safeguarding Lives', Hand Emplaced Munition (HENLM) Demonstration, Second Quarter, FY 2005, p2.

of the US subsidiary was quoted in 2001 as viewing MEMS technology being at the heart of their new mine replacement systems'.[8]

> "The system will use all kinds of remote and local sensors to warn you of an incursion. There will be a sensor field and you will be sitting miles away at your laptop and say 'Oops, we have an intruder.' It's very closely tied in with advanced sensor systems."

In practical terms this will mean that a virtual mine filed can exist in the circuits of a satellite which is remotely surveilling a target zone. Any 'virtual mine' triggered can launch a mortal salvo of either lethal or sub-lethal munitions.

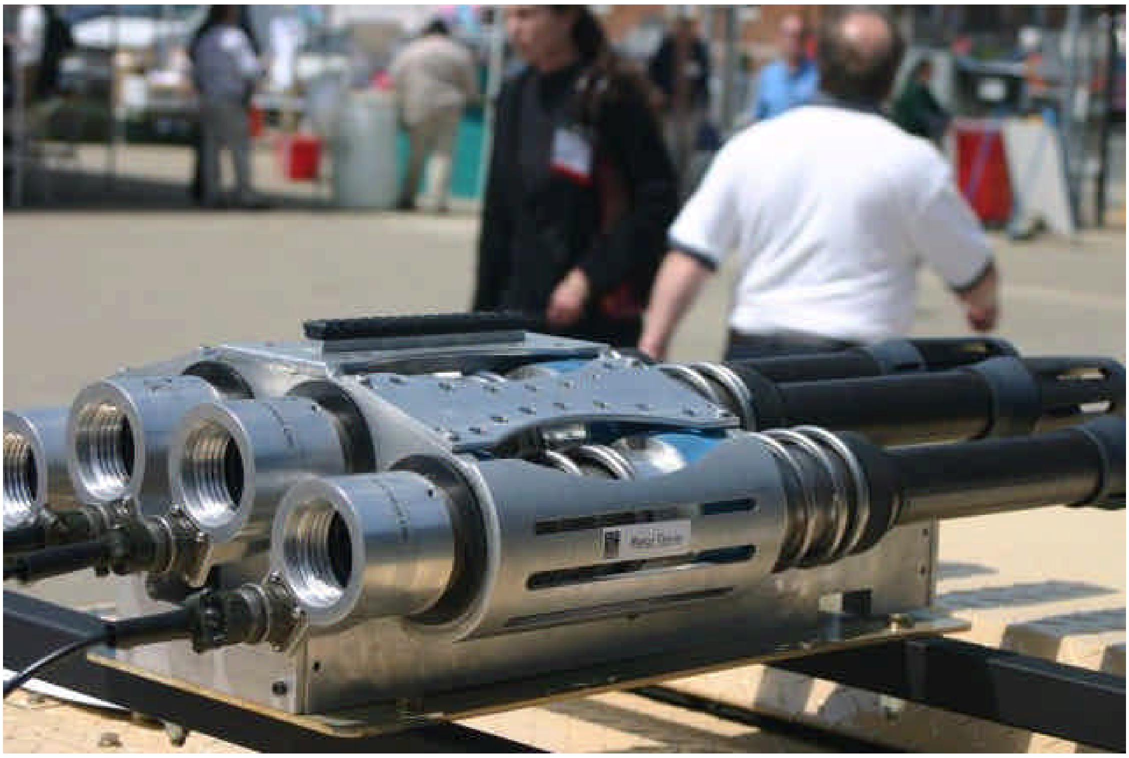

Figure 7: Metal Storm Mortars

[8] http://www.smalltimes.com/document_display.cfm?document_id=2101

Robotics

FPED is awash with robotic systems some of which were armed with both lethal and sub-lethal weapons such as the Scout, Matilda and MDARS and the Sword systems and equipped with night vision and laser range finders Others were essentially search tools with facilities for handling and destroying explosive devices such as the Iraq tried and tested Talon robot produced by Foster Miller and now owned by British company Qinetiq.

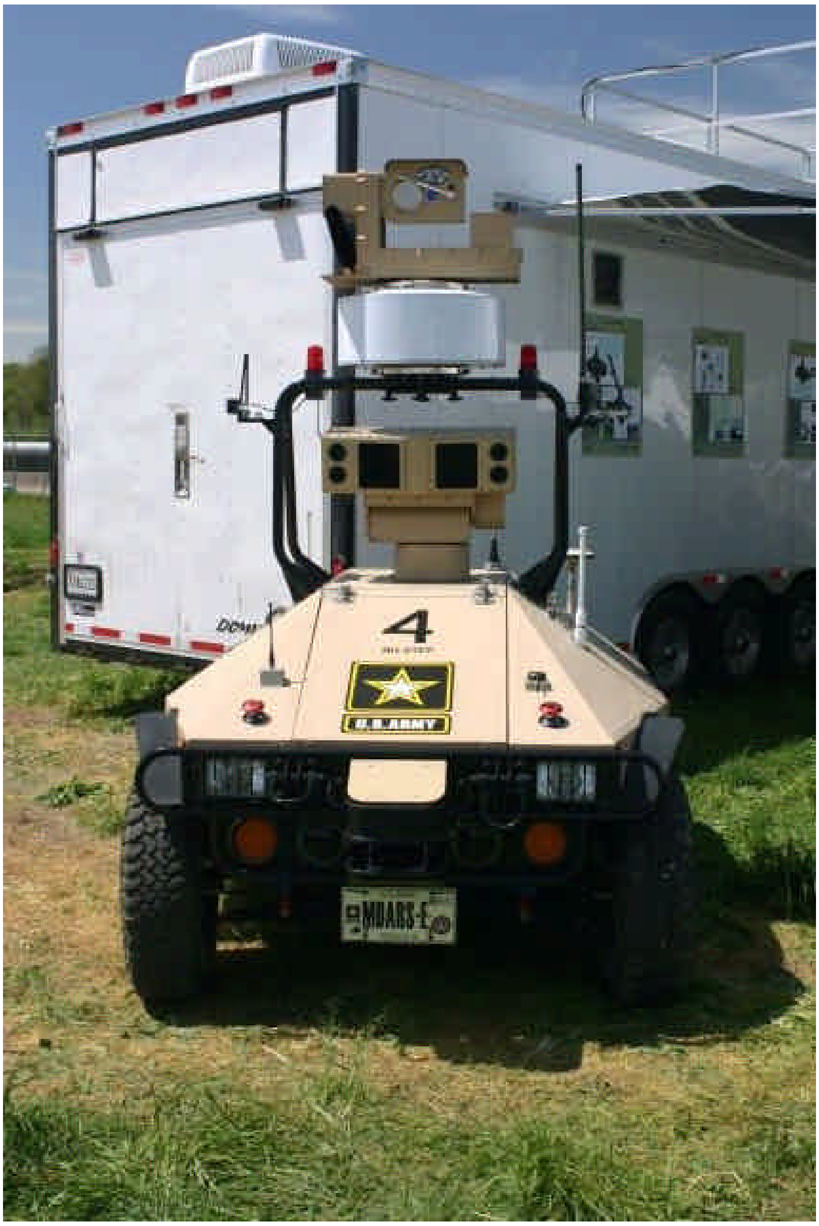

Figure 8: MDARS Robot on Display at FPED

Other Iraq mission-tested robots include some of Northrop Grumman's Remotec range that have acted as unmanned ground vehicles and armed sentries. Applied Perceptions are a company taking robots to a new level of remote control by fitting GPS systems for new extraction, evacuation, sentry and reconnaissance roles.

Whilst few would question the bomb disposal utility of robots such as the Andros on display here, concern should be raised by the advent of armed systems particularly if they become algorithmic or self-deciding patrollers. It's one thing to say they save the President from sending another letter of regret to the parents of human soldiers killed in action: but who is going to take a robot to a tribunal for violating human rights?

Unmanned Aerial Vehicles are another rapidly growing area of technology and were demonstrated at Quantico. The remote-controlled Aerial vehicle for the application of pesticides (RCAVAP) can carry a chemical payload which could just as easily be a riot control agent or a calmative weapon instead of an insecticide.

Target Acquisition – Weapons Sights & Systems

FPED is essentially a proving ground for advanced systems so it was no surprise to find a number of companies boasting of their superior target acquisition aids. These included telescopic sights for sniper rifles such as the precision optical sights manufactured by Cheytac and the image intensifiers produced by Simrad.

Figure 9a: Target Acquisition Aids

One entire corridor of this expo was filled with surveillance and target acquisition aids. They included infra red scopes from Raytheon and British Aerospace (offering 'uncooled Thermal Imaging Solutions for Homeland Security); laser illuminations systems for small arms by Insight Technology; Very long distance binoculars were displayed together with laser beam target designators which could either act as target designators which weapon systems could lock on to or as an accurate mechanism to map each potential target into a shared GPS system.

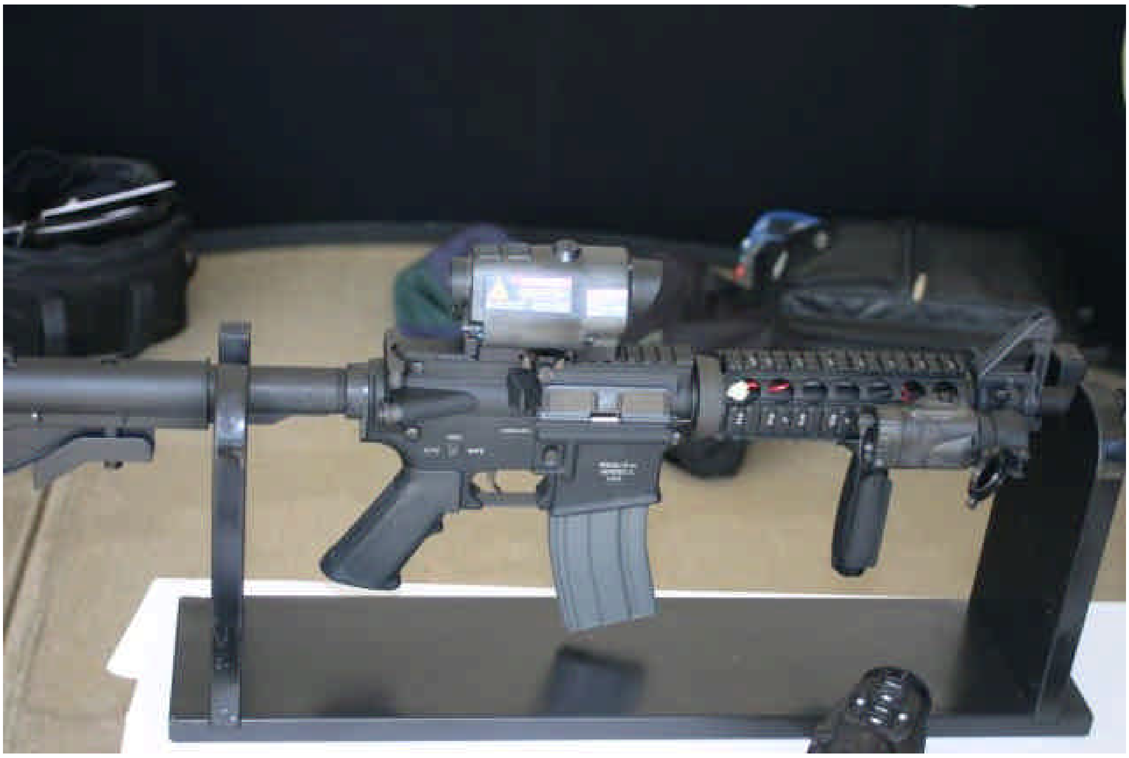

Figure 9b: Target Acquisition Aids

Perhaps the most James Bond like system on display was the Ibis 4 by 4, which looked like just another expensive SUV. However, this vehicle has a $100,000 pop up machine gun in its boot which could be target ranged and fired by a co-pilot using surveillance to lock on to any thing within a 360 degree circle.

Other novel sub-lethal target systems were also on display. Backed by the National Institute of Justice, mega corporation Raytheon was offering active denial using targeted directed energy beams. Versions were being prepared for Corrections, DoE, DoS, we were told. However if this system is ever allowed to be deployed in an algorithmic format as a self targeting pain beam, we are entering a new era of mass human rights violation.

Yet despite the hit tech gadgetry, the most sought after optics on the ground remain close combat optics. NDIA's National defence magazine reports that US Army's rapid fielding initiative (RFI) is buying 10,000 close combat optics a month to send to soldiers in Iraq for basic street patrols.

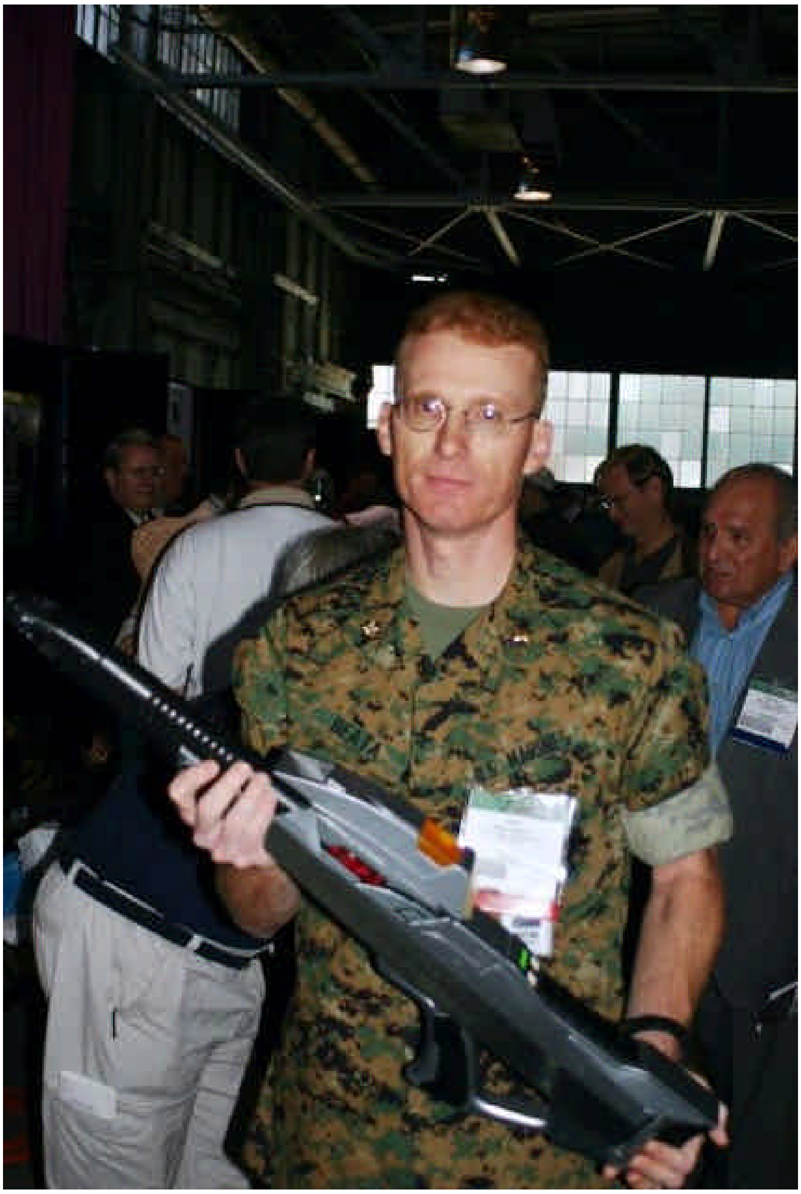

Figure 10: Mock-up of Handheld Microwave Weapon

Zone Monitoring & Clearance

A wide range of protective surveillance technology was on display including items such as the LKMD motion detector which can alert soldiers to any intrusions. On a wider scale, Qinetiq have created Cerberus which is an underwater swimmer detection system.

Other systems include a product from the NIJ's Border Research and Technology Centre (BRTC) called Bordertrack. This system which includes a laptop, GPS and laser range finder technology, can accurately track and map a range of activities in and around borders.

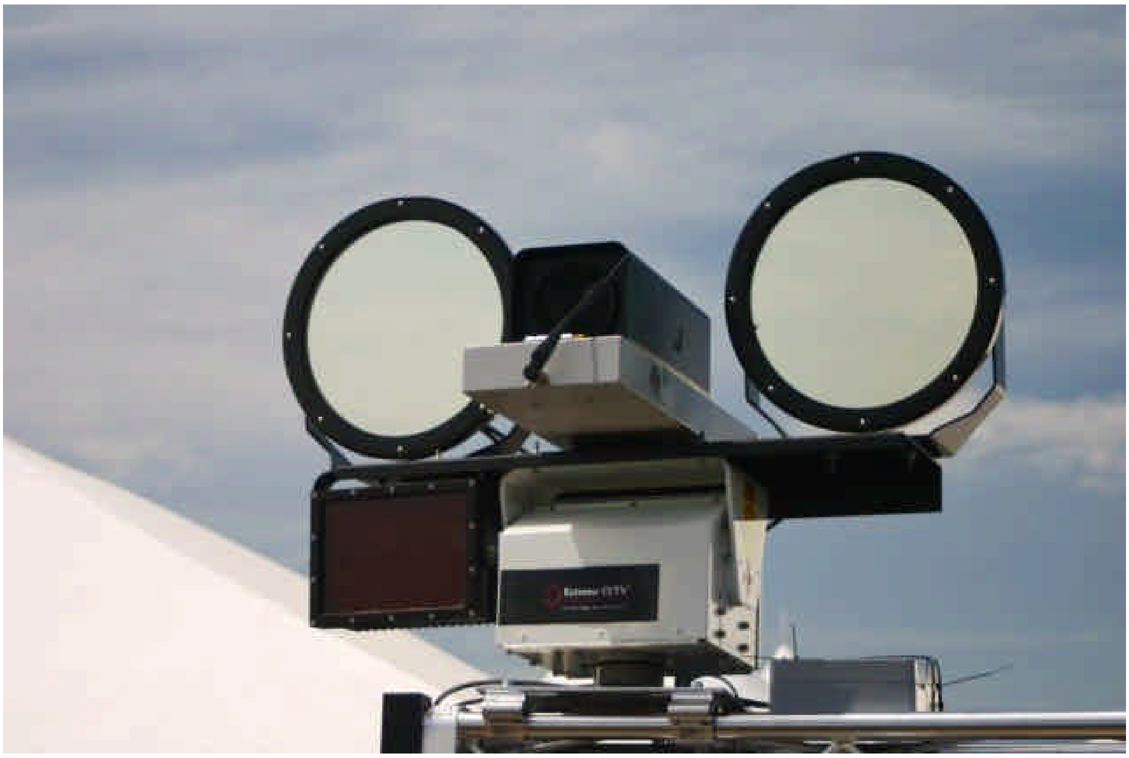

Figure 11a: Military CCTV Systems

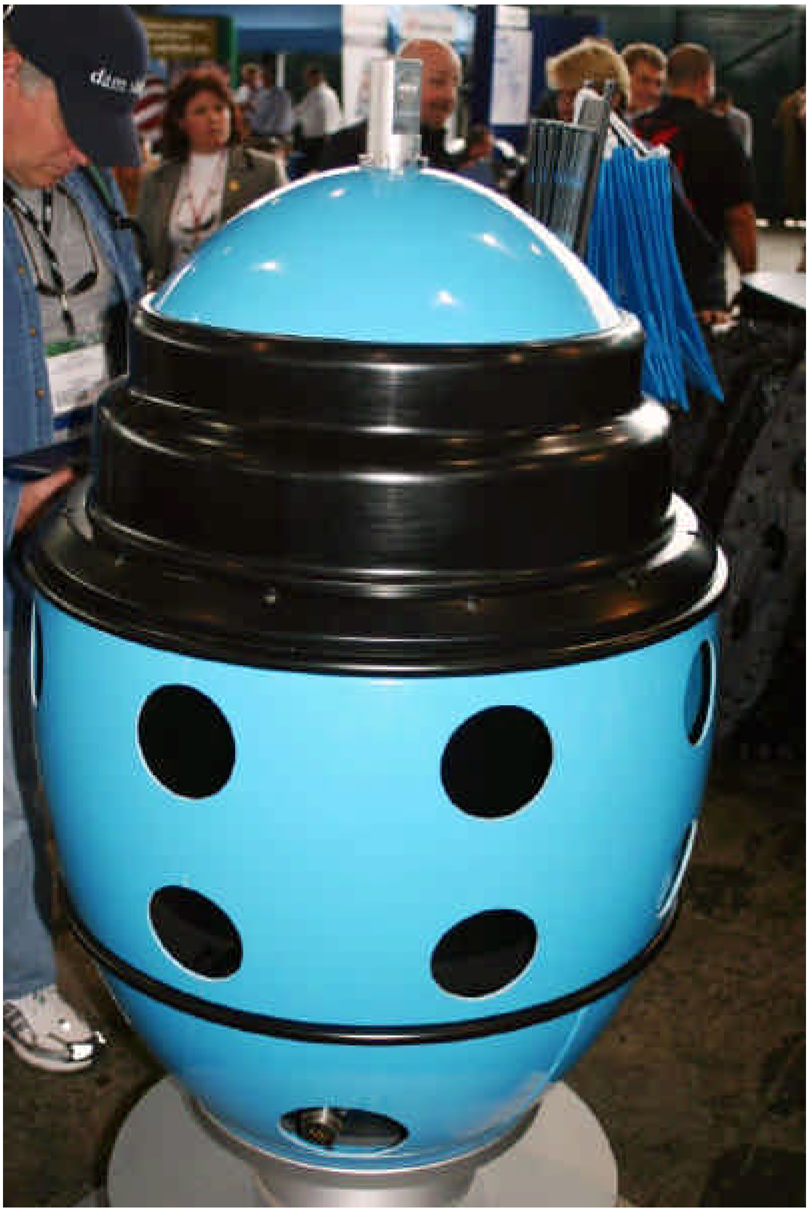

Figure 11b: Cerberus Swimmer Detection System

FPED showcased a substantial collection of high quality and performance surveillance systems. These included Precision Engineered Opto-Electronics Extreme CCTV systems. Indeed many of the products displayed here looked familiar from civilian usage but were much larger in both quality and performance. Pelco were there too, using the image of the Statue of Liberty.

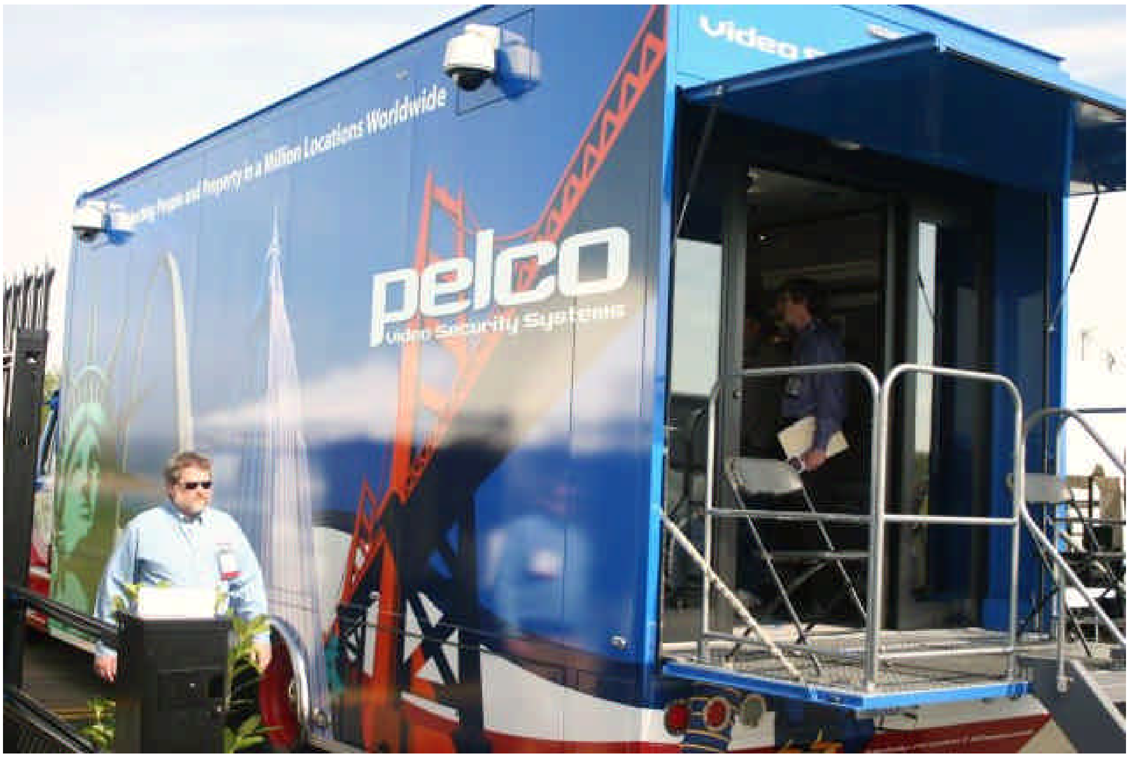
Protecting People and Property in a Million Locations Worldwide
Pelco
Video Security Systems
Video

Figure 12: PELCO Surveillance Stand

The salesman looked somewhat bemused when I reminded him that Amnesty International accused the Chinese of using Pelco cameras (subsequently replaced) in the Tiananmen Square massacre and broadcast the footage as wanted posters with a reward on primetime TV to catch students who participated.

The Department of Defence ‘Physical Security Equipment Action Group’ had a comprehensive programme of devices under development for ‘human presence detection and assessment; intruder detection from robotic platforms; perimeter security radars; remote detection and tracking sensors up to 5 km to name but a few.

Identity Recognition & Biometrics

FPED is a clearing house for information concerning new products and initiatives. For example newsletters from the National Law Enforcement and Corrections Technology Centre reported on the Referencing Ballistic Imaging Database (RBID) which enables rapid surveillance of ballistic fingerprints of weapons on file.

The US Department of Defense reported at FPED on the success of a hand geometry biometrics sytem at the Scott Air Force Base as an access control system through the Shiloh Scott Metrolink rail station entrance. In the wake of 9/11 base security has been a high priority and a number of related innovations were on display including the Advanced Vehicle Identification System (AVIDS) which can read English and Arabic licence number plates.

The US Homeland Science and Technology also reported on an initiative of the Biometrics Management office that awarded Lockheed Martin a contract to maintain the DoD ABIS and ensure it is compatible with the FBI's AFIS database.

There was even a ruggedized handheld biometric computer on show by MobiD solutions. MobiD's two mega pixel camera has been teamed up with Neven Vision to provide 2D facial recognition. It also incorporates a Fujitsu fingerprint sensor to capture images that are subsequently processed using the Cogent algorithm. Taken together the company boasts that the device has the ability to do either 1 to 1 matching or 1 to many identification. A voice recognition add-on is planned for 2005..

Security Screening

Some very advanced products were on display at FPED V including American Science and Engineering Inc.'s backscatter Xray products which can remotely scan buildings, vehicles and people.

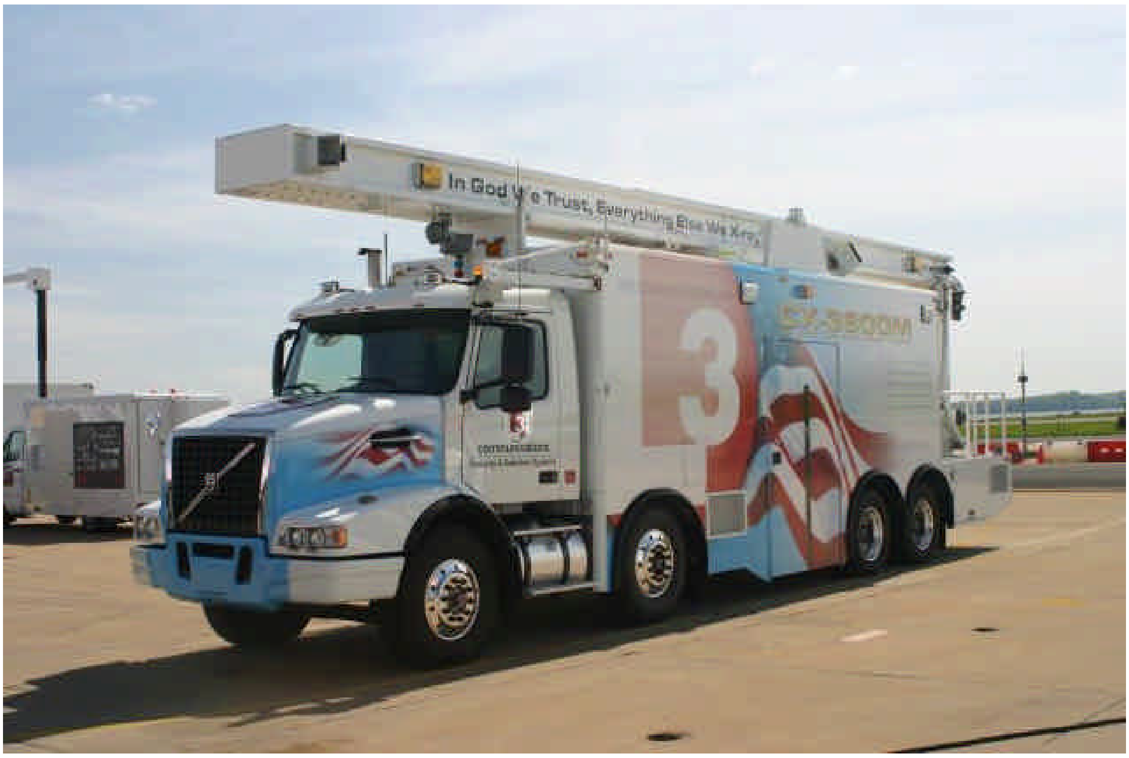

Figure 13: "In God We Trust, Everything Else We Xray"

Not all of the surveillance products had a killing vision purpose either – some were there for direct and in remote telemedicine. One of the most remarkable systems on display was the Sharp Systems 2nd. Generation 3D laptop based ACtius AL3DU, which enables 3D visualization without glasses. Using a standard surgical camera, the system produced a realistic crystal clear 3D view which would be a tremendous boon to surgeons in the field removing shrapnel or giving directions to medical personnel from further afield.

One company ‘smokecloak’ took the idea of security screening to a new and literal level by rapidly cloaking an entire zone with artificially created fog. Only those with IR vision can find their way through and that is presented as a significant tactical advantage over illicit intruders.

The mass surveillance of a wide range of threats was a key selling point for much of the technologies on display at FPED V. Thus ‘Federal Signal Corporation presents live demonstrations of all hazard warning solutions to ensure you are always prepared, including :wide area alerting; mass notification systems(MNS); personnel alerting systems (PAS); Visual security and monitoring.

Do such broad comprehensive monitoring packages actually work? – well not always….The President, who can afford to buy the best was banjaxed by a new security radar protecting the white house just as FPED closed. The system forced the President to flee to a security bunker when it misinterpreted dense cloud for an incoming missile. Nevertheless with Al Qaida seen behind every cloud and smokescreen, this military surveillance business is bound to boom.