19th International Congress on Modelling and Simulation, Perth, Australia, 12–16 December 2011
http://mssanz.org.au/modsim2011

The need for enhanced and coordinated video and imagery recognition surveillance systems

K.G. Webb

Truscott Crisis Leaders
Email: kwebb@crisisleaders.com

Abstract: Over the past seven years, and on behalf of the Australian Research Council (ARC) and the Government's Research Network for a Secure Australia (RNSA), the author completed doctoral level research and subsequent monitoring of a myriad of systems and methods for national security in Counter-Terrorism (CT). This involved personally interfacing with selected and knowledgeable national security personnel around the world, and maintaining personal contact with key Australian CT parties.

Aside from a number of other findings, and using the widely publicised experience of the effectiveness of visual surveillance in London following the terrorist incidents there in July 2005 as the catalyst, the results have shown that Australia needs, and would be wise, to enhance its national video and imagery recognition surveillance system.

Also, even though the research and subsequent monitoring has relatively restricted itself to Australia, it has shown that both nations and 'corporates' in general around the world need to do so. Particularly, those with isolated assets and/or exposure to potential major crises.

Exacerbating this is the:

- increasing pace of the 'Information Revolution';
- increasingly critical reliance on communications by friend and foe for their effectivenesss; and
- identification of terrorist parties with high technological capabilities, who are no longer restricted to conducting an act of terror in the ways that today's societal cumbersome and overbearing/impersonal security systems have been constructed.

The above implies the increasing need for a system that readily identifies changes and notices abnormalities, rather than just personal identification, and then disseminates such appropriately.

To sustain our future we need to design a blueprint that enhances, integrates, introduces, and consolidates automated real-time and post-event system capabilities across differing quality and disparate data sources. Thus the need for modelling and simulation.

This blueprint will need to provide three requirements. Namely, an:

- improved capability to visually recognise and alert on possible terrorist incidents;
- improved ability to identify and track individuals and objects; and
- enhanced content retrieval and analysis capabilities for data received.

Research to formulate the plan is currently underway around the world, thereby recognising the need. Particularly, in the UK where it has been progressing following the crime and terrorist acts of the past few decades, and where the effectiveness of surveillance has become quite evident in mitigating the risk.

The research is investigating the problem situation, identifying requirements, assessing relevant technology efficacy and strategically designing an automated smart surveillance system blueprint that can be:

- implemented within a reasonable time-frame, e.g. five years;
- used by whole-of-government to prevent, prepare, respond and recover from any terrorist and associated activity;
- accessible and partly used by selected corporate bodies and key installations/infrastructure; and
- achieved by jointly working with project partners already conducting similar in other parts of the world.

It can only achieve this with a proper international research project, which includes modelling and simulation; and, using the Author's personal research and monitoring to help Australia combat terrorist groups as its basis, this paper provides some background so what is necessary can evolve.

Keywords: *National Security, Counter-Terrorism, Surveillance, Video and Imagery Recognition, Intelligence.*

1. INTRODUCTION

A research project and subsequent monitoring investigating how to better manage national security from asymmetric threats, particularly terrorism, has identified areas requiring immediate research. One of these areas is the need for an enhanced national video and imagery recognition surveillance system. This is one that 'drills down and up', primarily through coordination, to all the critical parties operating within such a system and their sub-systems.

An example of the present situation, and not much has changed since 2004 when it was portrayed, is Figure 1 below. It provides a broad overview of the significant effect to mitigate acts of crime and terror that video and imagery analysis can now have in a purely crowded place scenario. It also gives some scope into the advent of recognition and surveillance technology over the past decade.

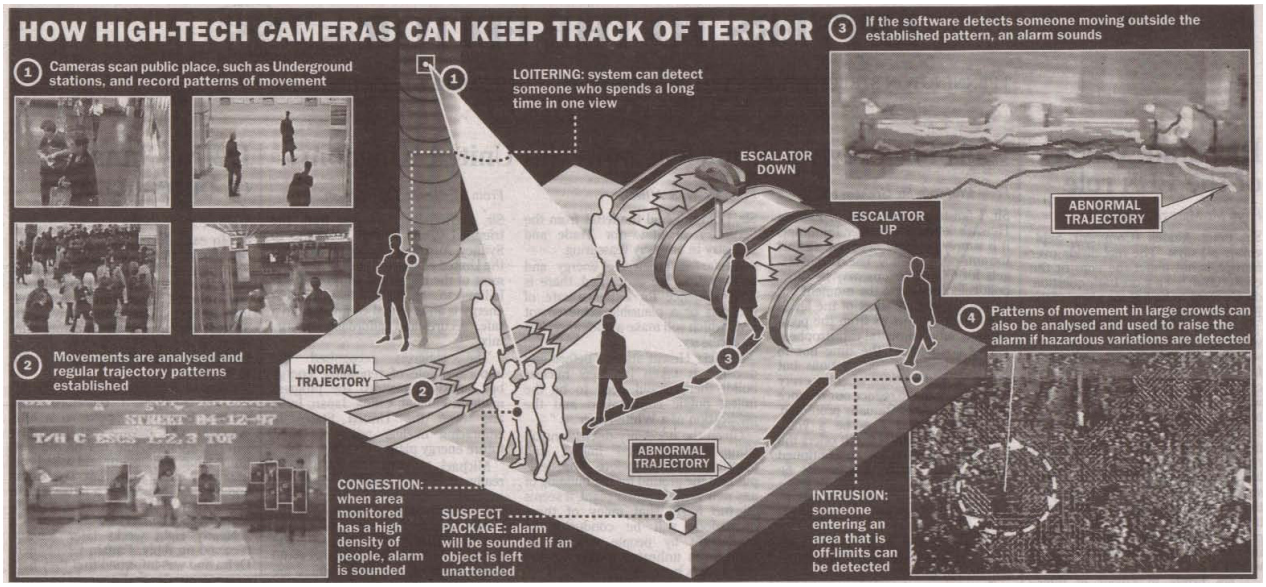

Figure 1. Examples of how video and imagery analysis can be used to counter terrorism (Ford et al, 2004)

However, despite the pictorial representation of a significant advancement in technology for security surveillance, the main issue still applicable today is that it is driven by hardware rather than analysis tools. As Lewis (2004) noted, 95% of effort has gone on hardware while only the remaining 5% has addressed analysis tools.

As publicly reported by Ford et al (2004), research into this commenced soon before the major 2005 terrorist acts in London, and it is fitting that nations work collaboratively with them and other parties to effect the same. This is particularly applicable when researching and applying the myriad of modelling and simulation requirements for any societal system.

Thus, the aim appears to be for:

- collaborative research into video and surveillance recognition that incorporates modelling and simulation,
- a smarter system that addresses the current issues and downfalls, and
- maximising the use and interpretation of technology for the desired standard of recognition and surveillance.

This paper outlines the reasoning and approach for a research project to achieve this, and an outline of some existing research in the area. This is so the intended and needed project, and the benefits/application of modelling and simulation within it, can be understood.

2. REASONING

2.1. Background

It is recognised that a deployment of sensors has now occurred, with technology such as hyper spectral and stereo imaging now commonplace. However, this needs to be leveraged through enhancing the technology and analysis of it further plus coordinating the systems it interacts with!

Accentuating this observation is that a British Home Office (BHO) Study in 2002 (Welsh & Farrington, 2002) identified CCTV reducing crime to a small degree, and that future CCTV schemes should be carefully implemented in different settings and employ high quality evaluation designs with long follow-up periods. It also identified that the systems should attempt to establish causal mechanisms for CCTV to have an effect on crime.

A similar study was then conducted by the BHO three years later (Gill & Spriggs, 2005) and it concluded that CCTV had still not been deemed successful. It emphasised that CCTV is not just a technical solution, as it requires human intervention to work best and the problems it helps deal with are complex. The study's concluding remarks stated that CCTV is a powerful tool that society is only just beginning to understand and a blueprint to use it is required.

Worth considering also is the media. The press reports and even the latest movies now show that the quest for advancing technology sensors has since become subliminally ridiculous.

A past example is the proposed 'see-through clothes' scanner (millimeter wave), which was to be deployed on London's underground system. It has now been put on the 'back burner', as its implementation appeared unfeasible due to many factors, such as the volume of traffic and physical constraints (Lettice, 2005).

2.2. Dilemma

In his presentation to the 2004 European Symposium for Defence and Security; Colin Lewis, representing the British Ministry of Defence (MOD), outlined the matters facing the 'dilemma' on security surveillance, which the Author has identified are still undergoing development today. The matters he mentioned included:

- End-user data collection and analysis,
- Zero motion detection,
- Event detection and classification,
- Abnormal behaviour recognition,
- Service activity monitoring,
- Vehicle monitoring, and
- People counting, tracking and recognition (Lewis, 2004).

Lewis (2004) expanded on this by explaining that the present focus by the British Government, due to its relevance and timeliness, is on:

- Imaging of people, luggage and cargo at the points of national entry/exit;
- Biometric imaging; and
- Detection of anomalous behaviour.

The following year, in 2005 after his presentation, the urgency of addressing these issues was highlighted when the major acts of terrorism occurred in London . Namely, CCTV played a key role in dealing with the bombings but there were over 2,500 tapes from tube stations alone required to be analysed, which meant a massive search process was needed to identify the perpetrators (Lewis, 2005).

In fact, research by the Author then and now shows the search process is still occurring to some extent, and this event alone confirms the requirement to enhance the system, and identify factors such as automation and the role of pattern recognition.

Confirming the seemingly required and being adopted shift of thinking in the UK back then is Simpson (2005), who explains that what is required is a focus on:

- Imaging as a basis for decision-making,
- Systems that are tolerant of a wide range of application scenario variations,
- Distributed systems,
- Dynamic reconfiguration of systems and ad-hoc networks (real-time variations in imaging capability and coverage), and
- Intelligence at a system level (localisation, distribution).

2.3. Constraints

The main sensory security technology behind this focus by the UK at present is biometric identification technology. While much of it is confidential and the operational contents cannot be disclosed, a good definition adopted by the main law enforcement agencies of biometrics identification is:

> *"The automated identification, or verification, of human identity through measurable, repeatable physiological and behavioural characteristics."* (PITO 2005, p. 36)

This form of technology has progressed from fingerprinting to DNA, and has now evolved into fringe technologies; such as body odour, ear geometry and keystrokes dynamics. Biometrics and ID management, e.g. multi-modal biometrics and 2-factor authentication, have also been identified as key technologies and trends in the cyber security space (Kearney, 2005). Therefore, it is clear the advancement in sensing technology has been profound and what is required is a system that properly and more efficaciously incorporates these advancements alongwith developing other areas that have not received the same focus.

Also, confirming this observation and the present situation are the actions by the US Government following the terrorist attacks in North America late 2001. Very shortly after this event, biometrics was embraced enthusiastically by US law enforcement agencies and within most levels of government. So why cannot other technologies receive the same focus!?

Other major constraints are often related to civil liberty and legislative issues rather than cost. The human rights issues in the US in particular are complex, mostly due to the federal nature of government, and differing perspectives between geographically and socially diverse areas of the population and legislature. However, the major incentive to those agencies countering terrorism is their willingness to accept guidance from the federal government and to have the ability to readily adopt and implement solutions with a minimum of bureaucracy (ITS, 2001).

Also worth considering and as Koger (2004 & 2011) explains, traditionally all the areas concerning surveillance have been plagued by complex issues based around managerial ownership and multi-agency responsibility, and these are often reinforced by discrete paper-based control systems and separate communications systems. Therefore, they have been purely 'platform-based', and even when computer systems exist they are often isolated from other related systems and tend to present supervisors with 'islands of data' rather than an integrated source of management information and intelligence. This infers a requirement to adopt a knowledge-based approach to an integrated surveillance system for national security from crime and terrorism.

The observations made above outline the current state of recognition and surveillance systems in today's society. As they show, the situation is quite dynamic and requires research to improve, which provides the reasoning for research into developing a blueprint that delivers this.

3. BASIC REQUIREMENT

Based on research conducted thus far by the Author and associates, a suitable design can be formulated for a national video and imagery analysis, recognition and surveillance system. When compared to existing arrangements, this is one that significantly enhances, integrates, and automates real-time and post-event system capabilities across differing quality and disparate data sources. Creation of such will mean an:

- improved capability to visually recognise and alert on possible acts of crime and terror;
- improved ability to identify and track individuals and objects; and
- enhanced content retrieval and analysis of video & image data recorded previously.

The Research Project proposed in this paper will meet this requirement by concurrently:

- reviewing leading-edge research in computer vision and image recognition technology;
- interacting with customers, actors and owners of the intended system; and
- engaging suitable systems engineering design methodology.

Many agencies responsible for national security expressed a requirement for such during the CT research project and subsequent monitoring conducted by the Author. Consequently, these agencies are expected to provide support in-kind by encouraging interaction with selected managerial and operational personnel to ascertain their specific needs, and thus alleviating this limitation. This will involve assistance in planning, access to key personnel and referrals to potential technology partners not already identified by the project team.

To protect the research project team's neutrality and to ensure bias in the design is minimised, financial support from users will not be sought. However, depending on circumstances and any specific demands that are over and above project plan expectations, a requirement for user in-kind contribution may develop.

4. RESEARCH PARTNERS SELECTION

4.1. Where to Look?

Research partners need to be those who show a great interest in what companies have to offer in terms of developed component solutions, which often incorporates their technologies also. This gives the advantage of, in a 'defacto' way, accessing such in technologically advanced countries and strong allies of the research partners.

Similarly, it is also recognised that the state of academic research and support is generally healthy and well supported by government and industry in most countries. The necessary research being proposed here, including modelling and simulation, can be spread across tertiary, government and industrial sectors. Plus, the importance of academic research as a supporting element of both industry and government is an accepted norm.

It is also important to note when selecting research partners that the USA itself should not become a 'given' primary research partner source. This was confirmed by the USA themselves when its own commission into national security/21st Century identified in their Phase III report (2001, p. 31) that "new classes of defense-relevant technologies are developing in which the major US defense companies and national labs have scant

experience. There are far fewer institutional linkages between government scientists and those innovative businesses generating and adapting cutting-edge technologies (e.g., genetic engineering, materials science, nanotechnology, and robotics)". Research by the Author shows that it is still addressing this shortfall.

Worthy of recognition on where to look for selection is the European Union (EU). It is engaged in a number of projects in this area, which increases access to the knowledge required by a nation such as Australia. An example is an EU-funded project for a distributed surveillance system that improves security in public transport networks and uses major networks in Europe as its test sites (Velastin et al, 2002).

Of note and indicative of the type of knowledge that the research project can discover if looking for partners in the EU is that ,'early in the piece', the proposed research project identified the following, which shows the 'hallmarks' of the findings:

> *"In terms of personal security, one of the main tools available to public transport networks is extensive CCTV (Closed Circuit Television) systems. The stated rationale is that the ubiquitous presence of cameras will deter potential offenders, reassure passengers and that events that threaten safety or security will be dealt with in a timely fashion. However, the main limitation in the deployment of effective CCTV surveillance systems is the cost of providing adequate human monitoring cover for what is, on the whole, a fairly tedious job. It is not rare therefore to find installations where the ratio of number of cameras per human observer is 20:1 or even larger. Consequently, CCTV tends to be used as a "reactive" tool (reacting to events as reported by other means)… It is clear that what is needed is a "pro-active" approach whereby the likelihood of events can be recognised more or less automatically so as to select useful quality information to human operators in charge of managing a transport network. It is therefore useful to replace routine human monitoring with computer vision systems able to detect events of interest."* (Velastin et al 2002, pp. 209-210)

4.2. Already Identified

A specific project partner working on such research has already agreed to partner in the proposed research. While they request not to be specifically identified via this means at present, it is important to recognise that the partner is a member of the UK's Imaging Technology Knowledge Transfer Network and consultant to a consortium set up to investigate CT capabilities for the British Government.

The partner has been working closely with the UK Home Office, MOD and Department of Trade and Industry (DTI) to review and report to Government on what is achievable using existing technology, and what needs further research in this area. They are already actively and directly involved in advising government agencies, industry and the research community on knowledge transfer of advanced image analysis techniques for use in security and policing applications, and indirectly through its knowledge transfer network, and academic and industry collaborations.

This work includes research, development and trialling of computer vision software solutions, that includes modelling and simulation, at major British airports for the detection, analysis, and recognition of:

- prescribed events,
- people and vehicle movement, and
- behaviour.

The collaboration partners include the British Airport Authority and Queen Mary University of London; and is being sponsored by the Home Office, DTI and the Engineering & Physical Sciences Research Council to develop novel and advanced image and video analysis technology. This means extensive experience in identifying, managing and delivering outcomes in research based technology projects, specifically in state-of-the-art computer vision applications. Particular experience includes but is not limited to:

- automated registration and alignment of biometric face recognition from live CCTV;
- holistic body language/gesture recognition/facial identity and behavioural recognition in CCTV video;
- intruder abnormal behaviour recognition and prediction in CCTV video;
- semantic content analysis including topic spotting, scene change detection and tracking in CCTV video; and
- incident, event and behaviour based video indexing, search, retrieval and analysis.

5. PROJECT APPROACH AND DESIGN

5.1. Approach

It is intended that the project will:

- investigate the problem situation, identify requirements, assess current and ongoing leading edge research and relevant technology efficacy in computer vision based image analysis and people and object recognition; and
- formulate a design for an automated smart surveillance system that can be implemented within five years and used by government agencies to prevent (where possible), prepare, respond and recover from any terrorist and associated activity.

It will achieve this by jointly working with project partners already involved in similar work and with a project partner that manages a collaborative network of CT researchers.

5.2. Design

The project will be conducted over 4-5 years and will incorporate analysis of a range of technologies associated with CCTV, video recognition, computer science and communications for a suitable system design that integrates with existing agency systems and methodologies.

It is expected that a key aspect of the design will be to use advanced image analysis techniques to inform remotely accessible and open architecture visual surveillance systems. This will occur by using networked CCTV at user defined locations that are capable of detecting, segmenting and recognising activity and objects such as people, luggage, vehicles and related movement; and record information captured by such systems (and other security sensors) in near real-time. Such systems will need to integrate with existing surveillance and IT infrastructure, as well as being used as a standalone turn-key solution for specific events.

Investigations will also address artificial intelligence and automatic learning to adapt to changes in the environment and situation to permit prioritisation of these observations. This is so that, once suitably configured and trained, the system can automatically trigger alerts for user defined events and bring the most important security issues to the attention of staff at CT agencies and related coordination centres. The underlying system will also need to use a highly scalable and robust database to store recorded video and associated high-level semantic information over suitably large periods of time to permit trend and outlier analysis.

The Project will involve the research partners working closely together to collaboratively design a system blueprint and identify likely technologies, as they probably would have discovered many of the technology candidates already. It will also require a degree of project management and coordination familiar to the partners, plus some necessary travel between the locations and meetings with key parties. This will form the main non-personnel expense of the research.

Of note is that such a partnership allows a significant benefit to be obtained from the lessons learnt and advances in image analysis research and development undertaken already. This will be used as a basis for further modelling and simulation, and grounding a design for further enhancement through users incorporating additional technology available to them. The approach also accelerates the project time-frame, removes much of the ground work required and triangulates the design, thereby benefiting the project and outcomes.

5.3. Composition

The research will be completed by a small number of personnel. Already, two main researchers are former commissioned Australian military officers with extensive direct operational experience in all areas of CT and the groups currently conducting such; and the necessary engineering, unconventional warfare, information operations and intelligence gathering knowledge. They also have direct global relationships with many users and industry, including senior police, and can be supported where necessary by similar people still operational.

The main selection requirement for other researchers are people with a common purpose, and the necessary experience, knowledge and desire to improve the ability to counter crime, including terrorism. This includes trying to involve industry wherever possible to become potential providers.

Due to its nature and the partnership, the Author believes the project has a very strong likelihood of success and can be completed within a five year period. It will offer a new capability that provides a significant edge to dealing with national security, major crime and countering terrorism.

6. PROPOSED R&D ADOPTION AND BENEFITS

The Project will deliver a new capability to counter-terrorism and associated agencies by providing a more robust, effective and efficient surveillance capability that uses real-world applications under sub-optimal conditions. It will enable non-intrusive ('covert') visual surveillance to be performed that:

- is not possible with existing manual techniques using CCTV,
- enhances the operations and collaboration of CT operators, and
- provides greater situational awareness.

This means, once implemented, these operators will have the opportunity for greater access to and knowledge of the situation, thereby making them smarter in dealing with the never ending threat.

The intellectual property of the system blueprint itself will rest with the research partners but the intellectual property of the tools within it will remain with owners and/or suppliers.

Research shows there are no similar products or options in their entirety already available on the market, as the current approach is very piecemeal and fragmented with users attempting to develop their own secular systems. They do not include a practised and unified system that allows simple collaboration and minimises resources. They also do not have direct access to a unique set of available technology and relationships already within the proposed research team, and this will only increase as suitable main researchers join.

From an Australian viewpoint, the Project objectives meet at least one of the Australian Government's four national research priorities, namely, Safeguarding Australia. Within this it meets the priority goals of critical infrastructure protection, protecting Australia from terrorism and crime, and transformation of defence technologies. It will link all relevant users and supporting partners more efficiently to meet these goals and bring knowledge not directly obtainable into Australia from overseas.

7. CONCLUDING REMARKS

Due to the common purpose and joint approach of research parties in allied countries, and their established alliances with academia, government and industry, the research will:

1. enhance user links within and between allies;
2. form solid linkages between research institutes on CT technology; and
3. enhance linkages between research, government agencies, end-users, and industry internationally.

This will also include direct linkage input into the research and development of technology tools, and greater association with parties doing this internationally. Greater collaboration, suitability and sustainability will result from these linkages. Thus, ensuring success in implementing, maintaining and enhancing any system designed.

Most importantly, it will allow the academic field of modelling and simulation to develop and prove its worth in an area of society where it requires greater utility, thereby enhancing its practice.

A research project to enhance national security and establish long-term linkages to achieve this perpetually is required.

REFERENCES

Ford, R., Coates, S. & Bone, J. (2004, September 22). New CCTV will catch crooks before they act. *The Times,* pp. 17-18. London.

Gill, M. & Spriggs, A. (2005). *Home Office Research Study 292: Assessing the impact of CCTV*. London: Home Office Research.

ITS (2001). *Report: Government International Technology Service Mission to the US*. London: DTI.

Kearney, J. (2005). Cyber Security: *Scope of technology, applications and drivers for change.* London: DTI

Koger, R. (2004). Holistic Monitoring of Complex Environments. *Airport* 1: 2-3.

Koger, R. (2011). *Personal Conversations - Various*.

Lettice, J. (2005, July 11). Could the 'see through clothes' scanner stop London terror bombs? *The Register.* London.

Lewis, C. (2004). Smart Surveillance: Prospects for the Future. Optics and Photonics for Counter-Terrorism and Crime Fighting: *European Symposium for Defence and Security*. London: SPIE.

Lewis, K. (2005). Keynote Talk – the Role of Photonics in Imaging and Identification. *Sensing and Imaging for a Safe and Secure World Conference*. Cumbria: EPSRC.

PITO (2005). *Part 1: Identification Roadmap 2005 – 2020. Biometrics Technology Roadmap for Person Identification within the Police Service*. London: Police IT Organisation.

Simpson, R. (2005). Keynote Talk – Sensing and Imaging for Safety and Security Applications. *Sensing and Imaging for a Safe and Secure World Conference*. Cumbria: EPSRC.

US (2001). *Road Map for National Security: Imperative for Change. The Phase III Report of the U.S. Commission on National Security/21st Century*. Washington DC.

Velastin, S.A., Boghossian, B.A., Lo, B.P.L., Jie Sun, and Vicencio-Silva, M.A. (2005). PRISMATICA: toward ambient intelligence in public transport environments. *Systems, Man and Cybernetics, Part A, IEEE Transactions* 35(1): 164 – 182.

Velastin, S.A., Vicencio-Silva, M.A., Lo, B., Sun, J. & Khoudour, L. (2002). A Distributed Surveillance System for Improving Security in Public Transport Networks. *Measurement and Control* 35(8): 209-213.

Welsh, B. & Farrington, D. (2002). *Home Office Research Study 252. Crime prevention effects of closed circuit television: A systematic review.* London: Home Office Research.