



---

# Proceedings of the 2nd Australian Security and Intelligence Conference

**1<sup>st</sup> to 3<sup>rd</sup> December 2009**

**Kings Hotel,  
Perth, Western Australia**

**Published By**

**secau - Security Research Centre  
School of Computer and Security Science  
Edith Cowan University  
Perth, Western Australia**

**Edited by  
David Michael Cook  
secau - Security Research Centre  
School of Computer and Security Science  
Edith Cowan University  
Perth, Western Australia**

**Copyright 2009, All Rights Reserved**

**ISBN 978-0-7298-0679-4**

CRICOS Institution Provider Code 00279B

## Table of Contents

Defeating biometric fingerprint systems: An applied testing methodology <i>David J Brooks</i>	pp 1 - 9
Information overload: CCTV, your networks, communities and crime <i>Vandra Harris, Crispin Harris</i>	pp 10 - 18
Security Decay: An entropic approach to definition and understanding <i>Michael Coole, David J Brooks</i>	pp 19 - 27
Professional Intelligence Judgement Artistry: Some early observations <i>Jeff Corkill</i>	pp 28 – 32
Terror attacks: Understanding social risk views between Singaporean lay and security practitioners <i>Yam Hong Loo, David J Brooks</i>	pp 33 - 40
Consensual security risk assessment: Overcoming bias, conflicting interests and parochialism <i>Benjamin Beard, David J Brooks</i>	pp 41 - 47
Energy Security: An Australian Nuclear Power Industry <i>Geoff I Swan</i>	pp 48 -54
Firearm Forensics Based on Ballistics Cartridge Case Image Segmentation Using Colour Invariants <i>Dong Li</i>	pp 55-63

## Conference Foreword

Welcome to the 2<sup>nd</sup> *Australian Security and Intelligence Conference* proceedings. The conference builds not only on our inaugural conference held last year, but also from the *Australasian Security Research Symposium's* that were held annually for almost a decade. Combine these with the other parallel suite of conferences being held by SECAU and Security Science is demonstrating a rich and large body of knowledge. Nevertheless, Security Science is still a relatively unique area of focused study, encompassing risk management, security management and technology in the protection of people, information and assets.

Security Science is a developing academic discipline and the research articles contained within the proceedings builds on this discipline. As this proceeding demonstrate, the topics are diverse and span the spectrum of Security Science, including such areas as the artistry of intelligence analysis, social views of terrorism to modeling security decay and testing security equipment, to name just four of the many articles. Such research leads to new and exciting developments in Security Science that can be applied within the broad and diverse domain of national to corporate security.

All papers were double blind peer-reviewed before acceptance into the conference for publication. Of nineteen submissions, eight papers were accepted for publication. Nevertheless, such a conferences as this is not possible without willing volunteers who follow through with their commitment and I would like to take this opportunity to thank the conference committee, administrators and article reviewers for their tireless efforts in this regard. Please enjoy the research articles that are presented in this proceeding's; however, also be aware that SECAU continues to development and advance the domain of Security Science and we welcome external contributors to partner in this important and exciting avenue of research.

Dr Dave Brooks  
Conference Chair

### **Conference Organising Committee**

Dr Dave Brooks	Conference Chair	Edith Cowan University
David Cook	Conference Editor	Edith Cowan University
Professor Craig Valli	Committee Member	Edith Cowan University
Dr Andrew Woodward	Committee Member	Edith Cowan University
Dr Patricia Williams	Committee Member	Edith Cowan University
Jeff Corkill	Committee Member	Edith Cowan University

### **Sponsors**

Australian New Zealand Forensic Science Society  
Edith Cowan University  
Secure Systems  
Kings Hotel

# Defeating biometric fingerprint systems: An applied testing methodology

David J. Brooks  
Security Research Centre (SECAU)  
School of Computer and Security Science  
Edith Cowan University, Australia.

## Abstract

*Biometric access control systems are becoming more common and may be considered high-security, due to their ability to identify and validate that the person is who they purport to be. Therefore, such biometric systems are often installed into critical infrastructure facilities as a means to gain high security protection. To date, there has been considerable research into the effectiveness of biometric devices to recognise valid users and reject invalid users, and to develop standards for interoperability. However, biometric systems are vulnerable to many categories of attack and there has been restricted research into such defeat vulnerabilities.*

*This article presents an approach that applied a defeat evaluation methodology to three high-security biometric fingerprint readers. Defeat testing included both physical and technical integrity testing, considering zero-effort to adversarial complex attacks. Physical defeat testing resulted in the attackers being able to gain entry into the internal circuitry of all three readers, with two readers having their tampers bypassed and access gained to the output relay door locks. Technical integrity testing resulted in one of the readers being defeated with an enrolled 2-dimensional fingerprint spoof and one reader being spoofed by a 3-dimensional fingerprint overlay, with all live finger monitor being defeated. These results indicated a number of significant vulnerabilities in the three biometric readers, raising concern with such systems being applied within critical infrastructure.*

## Keywords

Biometrics, fingerprint, defeat evaluation, spoofing, vulnerabilities, critical infrastructure

## INTRODUCTION

Biometric evaluation has, in general, considered the ability of such capture devices to deny valid users or accept invalid users, referred to as False Rejection Rate (FRR) and False Acceptance Rate (FAR). Much of the research and testing has focused on these measures of biometric access control systems, with limited consideration of system vulnerabilities (Dunstone and Poulton, 2008). Biometric systems, due to their measure of a person's physiological characteristics, may be considered to provide high security access control. Such a view was taken by the Australian Federal Government, with their allocation of \$182 million to deploy such systems at the borders (Wilson, 2007). In addition, such systems are finding their way into many diverse access control solutions, to improve performance, deliver greater returns and extend applications (Crozier & Cochrane, 2009). For many critical infrastructure or high security installations, the ability of the access control system to provide a robust and reliable system is paramount. However, system factors such as FRR may not be as much of an issue in higher security environments.

There are many groups working on biometric systems, for example the Biometric Working Group, the International Biometric Foundation, the International Organisation for Standardisation Committee and in 2008, the US Government released a recommended registry of biometric standards (Moradoff, 2009, pp. 17-18). Nevertheless, such groups are in general considering biometric interoperability, based on developing standards and not necessarily considering vulnerabilities of such systems. As Mansfield and Wayman stated when considering biometric performance testing, there are many possibly more important testing including vulnerability and security evaluation (2002, p.1).

This article presents a methodology for the evaluation of biometric fingerprint systems, with a focus on defeat evaluation suitable for high security and critical infrastructure facilities. Biometric fingerprint were chosen as they are considered the most common form of biometric reader. Three commercially available *high security* biometric fingerprint systems were tested for a sponsoring Federal Government agency using this applied method. Such evaluation methodology was considered important, for example the Biometric Institute agenda is to test the claims of biometric manufacturers and produce a vulnerability assessment program (Crozier & Cochrane, 2009).

## BIOMETRIC ACCESS CONTROL SYSTEMS

Biometric systems comprise of many techniques to extract, process and compare biometric characteristics. According to Johnson (2004), there are two classes of biometric characteristics, namely physical (physiological) and behavioural; with these classes divided into such methods as voice recognition through to iris scanning (Smith, 2006). Within a security context, biometric may be considered the highest level of validation, based on the principle of *something you have* (card, token), *something you know* (password) and *something you are* (biometric). As these stages are applied (Figure 1), alone or as multiple identifiers, the view is that the system becomes more secure as "biometric

characteristics is the true identifier of a person” (Smith, 2006, p. 624). However, this may not be the case when considering such issues as false acceptance rate and other system vulnerabilities.

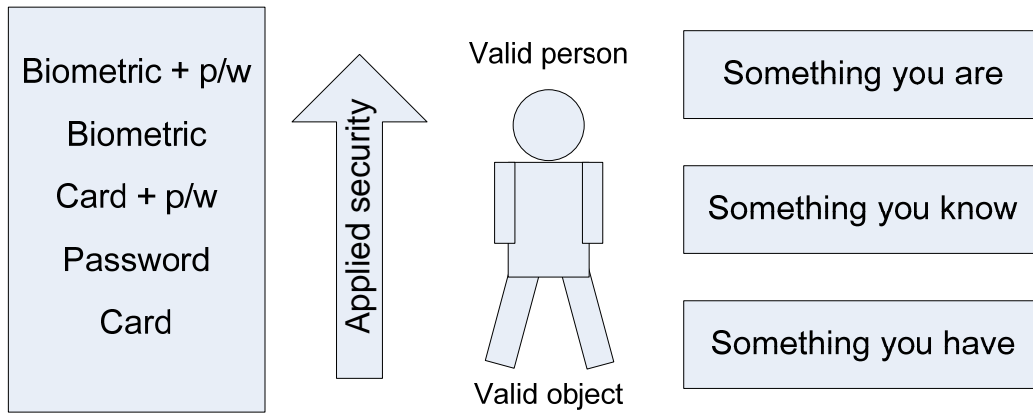


Figure 1 Levels of security access control

### BIOMETRIC VULNERABILITIES

Biometric access systems may be vulnerable to two different categories of attack, namely *zero-effort attack* or *adversary attack* (Jain, Ross et al., 2006). With a zero-effort attack the biometric traits of the attacker may be similar to a valid user, resulting in false acceptance (FAR) by the system. There may be a possibility that valid user templates stored in the systems database can be similar to that of the imposter, given the variance designed or defined into such systems. In an adversary attack, the attacker can imitate a valid system user by using physical or digital artefacts belonging to the user. The attacker can also change their biometric traits to match those of the system user.

In addition, there are other types of system attacks; circumvention, repudiation, collusion, coercion and denial of service. Circumvention is where the attacker may gain access into the system beyond that of the data collection plenum, peruse and modify these sensitive data (Jain, Ross et al., 2005). Repudiation is where an employee gains entry into the system and sensitive data, from which there may be circumvention by attacker (Rejman-Greene, 2001). Collusion is where the super-user modifies the system parameters to allow an attack to gain access to the system (Jain, Ross et al., 2006). Coercion is where the attacker threatens or blackmails an employee to grant him or her access to the system (Jain, Ross et al., 2006). Finally, denial of service is where the attacker floods the system with requests, which will overwhelm the system resources and deny the valid user access (Uludag and Jain, 2004).

These types of attack may be demonstrated within a systems approach (Figure 2), where up to eight attack points (Table 1) may be considered.

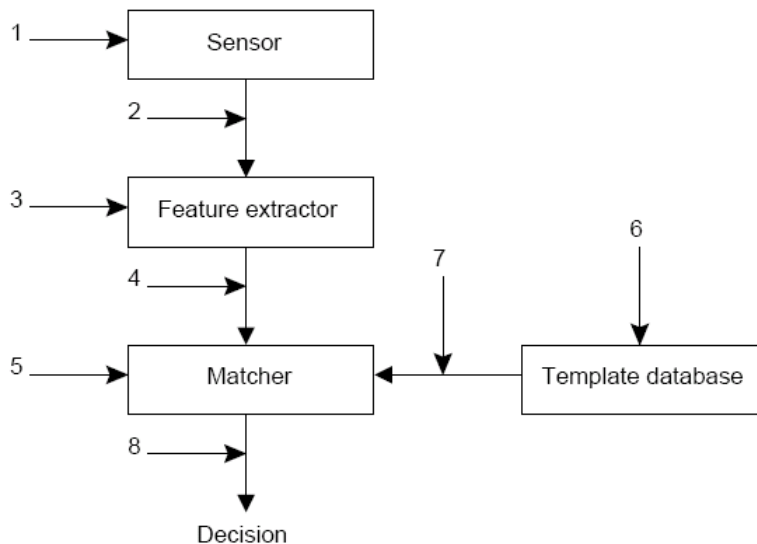


Figure 2 Generic biometric system attack points  
(Uludag, 2006)

Attack points	System components	Attack procedure
1	Sensor	Verification attack 2D or 3D
2	Data transmission	Data capture, injection, replay
3	Feature extraction	Fake data
4	Feature transmission	Fake data injection
5	Template matching	Template sensitivity
6	Database	Manipulated database
7	Data transmission	Manipulated data injection
8	Authentication	Matching data overridden or altered

Table 1 Biometric system attack points  
(Uludag cited in Smith, 2007)

In support, biometric vulnerabilities may have to consider three interrelated factors of the computing infrastructure, the human operators of the system and the specific biometric system (Dunstone and Poulton, 2008). The primary aim of defeat testing is to identify vulnerabilities in such systems and exploit these vulnerabilities. Such a view was supported by Smith (2007), who stated that such defeat testing seeks to exploit design and operational weaknesses in security systems to penetrate the security barriers.

### EVALUATION METHODOLOGY

The evaluation methodology applied a priori testing approach, which considered reliability, validity and testing scope. These three aspects were considered to be core principles during evaluation, an aspect raised by previous authors (Jones and Smith, 2005; Smith, 2007). *Reliability* ensures that tests are conducted in such a way that results are repeatable, given the same variables and environmental conditions. *Validity* ensures that tests should be based on a careful selection and isolation of independent variables, with the use of a control variable. In addition, that test's do evaluate what they assert to test. *Testing scope* includes simple to complex physical and technological attacks, resulting in an understanding of the systems vulnerabilities. Testing, in general, did not include attacks that were outside the scope of the device; such as attacks on external input/output devices, interfaces or communications.

A number of discrete steps were taken within the evaluation methodology (Figure 3), comprising of evaluation mapping, commercial evaluation, performance testing, defeat testing and resulting final report. These steps commenced with documenting a defined approach to evaluation, ensuring priori testing criteria and that proceeding stages are mapped. An approach that according to Jhistry and Frayssines is the first stage in formulating such evaluation strategies (2004). On completion of this first stage, the sponsoring agent's approval was gained to proceed to testing.

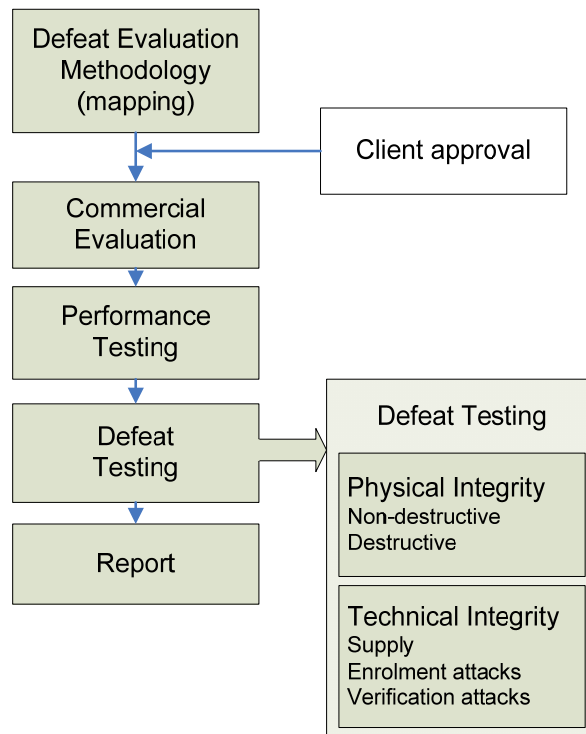


Figure 3 Biometrics defeat evaluation methodology

Commercial evaluation reviewed the robustness of manufacturer, supplier and logistics across all Australian states and territories. Reviews of national and international standards that may be applied to the test item were considered, with any past testing sourced.

Performance testing applied environmental testing on the device, with the prime intent to ensure compliance to manufacturer’s stated specifications. In addition, environmental testing included inclement weather, user interface issues, environmental noise, etc. With the biometric fingerprint systems the FRR and FAR - with a restricted population size - were applied, considering the defeat evaluation of zero-effort attack and with such conditions divided into three categories of false acceptance analysis, non-ideal user conditions and non-ideal interface conditions. The user interface testing was, where possible, a quantitative investigation into the device’s ability to accept *all* users under a range of non-ideal conditions.

Defeat testing was the main consideration within the evaluation and attempted to use both physical and technical adversary attacks against the device. These attacks included spoofing the device’s detection capability in an attempt to identify vulnerabilities. Physical integrity tested both non-destructive and destructive structural integrity, access to enclosure, etc. Technical integrity tested the power supply, the device’s underlying technology, tamper capability, etc. The evaluation was concluded with a comprehensive technical report of the testing results submitted to the sponsoring agency.

## DEFEAT EVALUATION

The evaluation of the device attempted to discover vulnerabilities that may allow an intruder to bypass the device without triggering an alarm. The evaluation is categorised as:

- *Physical integrity*: to determine the item’s physical resistance and vulnerabilities to attacks by covert and overt force.
- *Technical integrity*: to determine the item’s technical resistance and vulnerabilities to bypass attempts using both zero-effect attacks and adversary technological attacks.

### Physical Integrity

Physical integrity considered both non-destructive or covert attacks, and destructive attacks attempting to gain access into the device. Both approaches sought to evaluate the device’s physical protection against such low level technical attacks, noting system vulnerabilities.

#### *Non-Destructive Access to Item Interior*

Non-destructive evaluation examined the ease (or delay) involved in removing the device’s cover or otherwise opening the item’s enclosure to gain access to its interior. Methods considered techniques that did not damage the device or show external tampering, maintaining a degree of covert access. Testing considered whether it was useful to the intruder to access the interior of the device and if such an attack was possible without triggering an alarm. The use of laboratory tools such as fine-blade screwdrivers, Allen and star keys, razorblades and such were used in this test.

*Destructive Access to Item Interior*

Destructive evaluation examined the ease (or delay) involved in gaining access to the device’s interior using methods that may cause both superficial or destruction damage, such as forcibly removing the device from its mounting or piercing the device’s enclosure. If the device had any sensors present to detect such an event, this was noted and attempts applied to defeat such anti-tamper devices. Testing included, but was not limited to, practices such as hammer strikes, prying and drilling. The assessment included a subjective discussion of the quality of casing and connecting hardware. The destructive testing used laboratory tools such as large screwdrivers, hammers, drill and drill bits.

**Technical Integrity**

With the creation of a *key*, biometric readers assume that every fingerprint presented is a credential unique to that user. If anyone can present a credential that the system considers valid, the system is essentially defeated and this constitutes a systemic failure to reliably authenticate users. Failure may be simple or complex adversarial attacks. The attacker may imitate a valid user by using the physical or digital artefact belonging to that valid user. The attacker may also change their biometric traits to match those of the system user. Technical attacks considered the ability of the device to resist artificial methods of defeat, including supply attacks, enrolment attacks and verification attacks.

*Supply Voltage Testing*

The supply voltage was tested to simulate both high and low voltage supply and likely effects this may have had on the device (Figure 4).

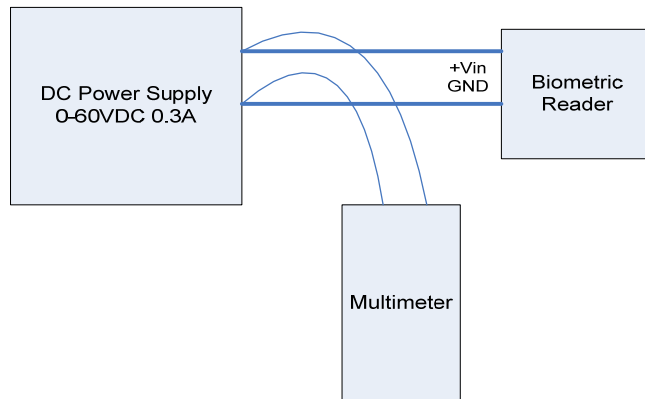


Figure 4 Supply voltage evaluation test

Commencing from the manufacturers specified voltage; the evaluation increased or decreased the device’s supply voltage by 2V increments. During each change in voltage, ten-fingers were presented for validation and any effect noted.

*Attack Analysis*

These tests examined the device’s ability to resist adversary attacks of a deliberate and sophisticated nature, divided into two categories of enrolment and verification attacks.

*Enrolment attacks:* attacks that attempted to undermine the principles and inherent security benefits of biometric systems by enrolling any of the artificial fingerprint types used in the verification attack testing. Due to the intent to consider defeat evaluation, enrolment tests were not applied.

*Verification attacks:* attacks that attempted to gain access during verification by using an artificial replication of a legitimately enrolled fingerprint. Verification attacks applied artificial replication methods, including both 2-dimensional types such as photocopies and photographs in various formats and media (Table 2; Figure 5), and 3-dimensional types such as residual prints on scanning platen, artificially constructed fingers and fingerprint overlays (Figure 6) on live fingers.

Photocopy	Photograph
-----------	------------

Black and white paper	Greyscale paper
Greyscale paper	Colour paper
Colour paper	Colour transparency
Colour transparency	Colour paper with depressed print
Water misting with above	Water misting with above

Table 2 Two-dimensional attack mediums



Figure 5 Artificial 2-dimensional depressed fingerprints

2-dimensional attacks: Several verification attacks with 2-dimensional images were attempted. The images were placed onto the platen 10 times, to see if the device would read the images. If the image was read, another 20 tries were conducted to ensure a proper read and rejection had been made. In addition, water misting was incorporated to replicate *live finger* monitoring.

The above adversary attack method was repeated with 3-dimensional medium. Artificial 3-dimensional fingers and finger overlays (Figure 6) were made from different substances, primarily Gelatine poured into various moulds such as moulding plastic or etched circuit boards. This technique followed past testers (Mansumoto, Matsumoto, Yamada, & Hoshino, 2002), who published their artificial fingerprint spoofing methods.

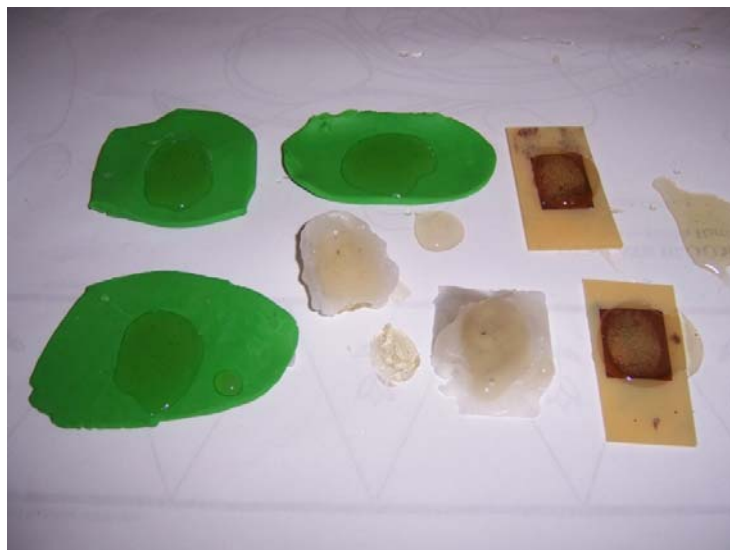


Figure 6 Replicated 3-dimensional finger overlays

**APPLIED DEFEAT EVALUATION**

The defeat evaluation methodology was applied to three *high quality* biometric fingerprint devices. Each item was supplied from different manufacturers and with various image scanning and capture techniques.

*Biometric fingerprint reader one*

The first biometric fingerprint reader device was supplied in two discrete components, namely the Platen Reader and Secure Input/output board. The platen used a Radio Frequency (RF) ultrasonic sensing device, contained within a metal housing. Image data captured from the sensing device is encrypted to the Secure Input/output board. The Input/output board contains the power supply input, reader interface, output relay and door open output.

*Biometric fingerprint reader two*

The second biometric fingerprint reader was supplied as one complete stand-alone device, which contained the biometric platen, RFID reader, externally LCD display, 12-button keyboard and internal circuitry attached to the metal chassis and hardened plastic cover. The fingerprint scanning platen operated through an optical sensor.

*Biometric fingerprint reader three*

The third biometric fingerprint reader was supplied as a complete device, which contained the biometric platen, RFID reader and internal circuitry attached to the metal chassis and hardened plastic cover. The fingerprint scanning platen operated through an optical sensor.

## **RESULTS**

The following defeat vulnerability results were obtained from the three biometric fingerprint devices.

*Physical integrity and vulnerabilities*

Evaluation comprised of both non-destructive and destructive testing. Simple physical attempts were made to pry the device casing from their mounts using a large screw driver. Various parts of the device were subjected to physical attacks, with a focus around the key fixing points. Attempts were made to crack or break the devices casings from its mount, using a medium weighted hammer and with various parts of the readers attacked. In general, 2 of the 3 devices proved to be robust in their ability to resist such brute force attacks. However, one of the devices could have its cover prised off with a screwdriver. Moreover, all three device's internal circuitry could be easily accessed with the use of common fixings. In one case, there was no cover tamper fitted. With the other two devices, the cover's anti-tampers could be bypassed with limited technical capability.

In two of the three devices, once access to the internal circuitry was possible this exposed the door release circuits. These circuits could be easily bypassed to active the door release, allowing door access. The third device came in two discrete components - platen reader and secure input/output board – with the door relay circuitry contained within this second component.

*Technical integrity and vulnerabilities*

Technical integrity evaluation included a number of 2-dimensional, 3-dimensional and multipoint attacks, leading to a number of vulnerabilities.

All three of the devices, when combined with water misting, would attempt a read of a 2-dimensional replicated finger. This misting approach also resulted in 2 of the 3 readers having a denial-of-service when water pooled. Nevertheless, none of the three items could be defeated with 2-dimensional replicated fingers. However, one of the readers allowed a replicated image to be enrolled and then read.

While the fake 3-dimensional fingers would trigger a read condition in all devices, only one of the three devices resulted in a false acceptance condition. The use of fake 3-dimensional finger overlays, on a live finger, proved to be the most effective method (Figure 7). In addition, this approach could prove to be the most covert, as such manufactured overlays were discrete and could be fixed to the attacker's finger.



Figure 7 3-dimensional replicated fingerprint overlays

All the devices suffered some degree of random false acceptance read (FAR); however, due to the irregular nature of these FAR these were not repeatable. Nevertheless, when considering the relatively restricted number of test reads and testers applied during the study, the devices FAR's were of some concern.

## CONCLUSION

The article has presented a defeat evaluation methodology for the testing of biometric systems, applied against three *high* security fingerprint reader devices. The evaluation methodology proposed a five stage process, with testing comprising of a commercial evaluation, performance testing and finally, defeat testing. Defeat testing was the prime focus of this evaluation, dividing this stage into both physical integrity and technical integrity. Defeat testing attempted to seek and examine vulnerabilities within the biometric devices.

Each tested biometric fingerprint reader device had some degree of vulnerability, with some of these being quite simple physical security failures. Physical defeat testing demonstrated that attackers were able to gain entry into the internal circuitry of all three readers, with two readers having their tampers bypassed and access to the output door relays. Technical integrity testing demonstrated that one of the readers could be defeated with an enrolled 2-dimensional spoof and one reader could be spoofed by a 3-dimensional false fingerprint overlay, with all *live finger* monitoring being spoofed.

The article has shown that biometric systems, although considered *high security*, can be defeated using various techniques. Therefore such systems, however technology driven, should be considered one component within a holistic critical infrastructure security environment, with layers of deterrence, detection, delay, response and recovery.

## REFERENCES

- Crozier, R., & Cochrane, N. (2009). *Biometrics: the ultimate security?* Retrieved August 6, 2009, from <http://www.crn.com.au/Tools/Print.aspx/CIID=149591>
- Dunstone, T., & G. Poulton (2008). *Biometrics vulnerabilities: a principled assessment methodology*, Sydney: Biometrics Institute Ltd.
- Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: a tool for information security. *IEEE Transactions on Information Forensics and Security*, 1(2), 125-143.
- Jain, A. K., Ross, A., & Uludag, U. (2005). *Biometric Template Security: Challenges and Solutions*. Proceedings of European Signal Processing Conference (EUSIPCO), Antalya, Turkey.
- Jhistry, S., & Frayssines, B. (2004). *Technical test methodology*. Unpublished manuscript, Perth: Edith Cowan University.
- Jones, D. E. L., & Smith, C. L. (2005). The development of a model for the testing and evaluation of security equipment within Australian Standard / New Zealand Standard AS/NZS4360:2004 - risk management. *Recent Advances in Counter-Terrorism Technology and Infrastructure Protection*.
- Mansfield, A. J., & Wayman, J. L. (2002). *Best practices in testing and reporting performance of biometric devices* Teddington: National Physical Laboratory.
- Rejman-Greene, M. (2001). Biometrics - real identities for a virtual world. *BT Technology Journal* 19(3): 115-121.
- Smith, C. (2006). Trends in the development of security technology. In M. Gill. (Ed.), *The Handbook of Security*. Basingstoke: Palgrave Macmillian Ltd, 610-628.

- Smith, C. (2007). The evaluation of security systems: Testing biometrics and intelligent imaging systems. *The 6th International Workshop for Applied PKC (IWAAP2007)*.
- Uludag, U. (2006). *Graduate psychology: Secure biometrics systems*. Michigan: Michigan State University.
- Uludag, U., & Jain, A. K. (2004). Attacks on biometric systems: a case study in fingerprints. *Proceedings of the SPIE-EI 2004*, San Jose.
- Wilson, D. (2007). Australian biometrics and global surveillance. *International Criminal Justice Review*, 17(3), 207-219.

## **COPYRIGHT**

David J Brooks ©2009. The author assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

## Information overload: CCTV, your networks, communities and crime

Vandra Harris<sup>1</sup> & Crispin Harris<sup>2</sup>

<sup>1</sup> School of Law  
Flinders University

<sup>2</sup> Security Consultant

### Abstract

*Electronic surveillance continues to play a central but often unobserved role in contemporary Western societies and attempts to police them. This paper focuses on closed circuit television (CCTV) footage and its technological implications, particularly relating infrastructure and data storage and integrity. While CCTV might appear attractive in augmenting law enforcement systems, the authors argue that the debate on use of CCTV in crime prevention remains incomplete without an effective understanding of the diverse costs. This discussion reveals startling ICT resource needs and associated costs, together with very specific technological capacity. These contribute significantly to the costs of such systems, reinforcing the authors' argument that CCTV is no golden bullet for law enforcement.*

### Key words

CCTV; data security; live streaming; law enforcement; policing

### INTRODUCTION

Closed circuit television (CCTV) systems collect video and direct it to a central monitoring system that may be monitored in real time or 'near real time'<sup>1</sup>, and/or record the video for later inspection or playback. There are four key aims of these systems in law enforcement: deterrence, rapid response, investigation and identification, and prosecution of crime. As technological developments in the last four decades have made CCTV cheaper, smaller and easier to operate, its use has expanded significantly, to the point that a European survey revealed that nearly one in three premises and institutions utilised CCTV surveillance in 2002 (Hempel and Töpfer, 2004, p. 3). As use has increased, so too has commentary on the effectiveness of the medium, its impact on society, and the attempt to balance the rights and liberties of 'the innocent' with the responsibility to protect them and apprehend 'the guilty'. This paper aims to balance that commentary with a clear understanding of the technological impact and requirements of such systems, to assist effective planning and decision-making regarding CCTV use for law enforcement.

A scan of Australian newspapers reveals that CCTV is popularly perceived as effective in deterring crime and securing convictions. Prior to the 2007 APEC Summit in Sydney, the number of CCTV cameras monitoring that city's public transport network was increased to 6,400, as a 'strong deterrent to common criminals and thugs' (NSW Acting Premier John Watkins, cited by AAP, 2007). Similarly, a more recent article in *The Australian* (Martin, 2009) stated that the showing of CCTV footage on news broadcasts acts 'as an overarching safeguard and deterrent'. This perception is not necessarily matched by evidence, and needs to be balanced with a clear understanding of the actual efficacy as well as the technological requirements of systems. Understanding this will contribute to the ongoing dialogue about the usefulness of this tool in an era of increased surveillance and shifting perceptions of a need to balance civil liberty and civic safety.

Our specific contribution to this debate concerns the technological aspects of CCTV, in particular the impact on technology and data storage requirements for enforcement regimes, notably by police. The paper commences with a brief explanation of the technologies we address, and the contexts in which their applications relate to law enforcement. We then briefly address the academic literature on the efficacy of CCTV in crime prevention and prosecution, before moving to our primary focus on the realities of data management arising from CCTV applications in mainstream law enforcement. This discussion includes attention to the question of whether CCTV is a cost-effective method, and whether technological resources currently available to Australian police forces are adequate for optimal use of CCTV tools. We note that significant investment would be necessary in the short term to ensure that police services can adequately manage the data arising from increasing CCTV application and to ensure that the technology meets the needs and expectations of these services. We conclude that while CCTV can be useful in a number of ways, the expectations must be well defined, and infrastructure impact must be carefully considered as a core component of the implementation.

---

<sup>1</sup> That is, within minutes of the actual events.

## TERMS AND TECHNOLOGIES

It is important to commence with a strong understanding of the terms and technologies in focus in this paper. CCTV cameras record individual images that together create a moving image. Most CCTV systems collect these images at a rate of over 15 per camera per second. Individually, these images – or ‘video frames’ – are smaller than most commonly available images (less than 16Kb per frame)<sup>2</sup>. While the individual images are small, the collection of this information for later playback can add up to a substantial amount of data: one camera recording low quality video for 24 hours at this rate will record at least 1.3million images, generating over 20Gb of video (equivalent to 5 movie-length DVDs).

‘**Streaming**’ of data refers to the practice of sending a constant flow of data (usually audio or video) over a data network to a remote location, and ‘live streaming’ refers to transmission of this data at the time that it is captured. In practical application, live streaming of CCTV is the exception rather than the rule – video is usually recorded for later reference rather than being monitored immediately. Banks, for example, store CCTV footage at branches rather than centrally, due to the volume of data created by 16-32 cameras per branch, generally recording higher quality (and thus larger) images than those described above. Such a high volume of data would require significant bandwidth for transmission, but in this case identification *after* the fact has been deemed sufficient when combined with other security mechanisms.

Live streaming is usually used for transient data (that is, data that will not normally be stored after viewing) and in most cases involves the transfer of high volumes of data. Examples of cases in which live video streaming may be applied include internet broadcasts of sporting matches and the NASA ‘net-cast’ space shuttle launches<sup>3</sup>. In crime prevention applications, CCTV footage is streamed to enable live monitoring of locations or events as they occur. An example of a substantial, actively monitored CCTV system is a public railway network: metropolitan rail networks frequently have over 5,000 cameras and are actively monitored by railway police in a central location. Where data is not streamed, it is stored on the site of collection.

While CCTV **system sizes** vary, a regular ‘off-the-shelf’ system (which can be sold as a pre-packaged bundle or in separate pieces) generally comprises up to 16 cameras<sup>4</sup>. Systems of this size would be appropriate for a small to medium business with a single physical location, and includes approximately a terabyte<sup>5</sup> (Tb) of local storage (adequate for seven days of recorded data) and dvd burner to allow data to be recorded for review. As will be discussed, both storage and transmission of this volume of information can involve substantial financial investment (including conversion equipment, storage space and systems that enable later retrieval of data). Public space systems tend to be many times larger than this, as in the case of the rail network referred to above.

## LAW ENFORCEMENT APPLICATIONS

Where CCTV is used for surveillance it is rarely a police operation: private enterprise or different levels of government frequently install and/or monitor cameras, either exclusively or in partnership with police. According to Wilson and Sutton (2003, p. 2) ‘the push to establish CCTV in Australia has come from local government’, and this diversified ownership and responsibility has particular implications that will be expanded below. Where CCTV is used in crime/incident investigation (to assist investigations into crimes that have already occurred), the video is generally sourced from non-law enforcement CCTV systems such as these. It is therefore not useful to limit this discussion only to police-owned and operated CCTV systems.

Nonetheless CCTV is used in a diverse range of law enforcement contexts, for one or more of the four purposes listed above (deterrence, response, investigation and prosecution). Live-monitored CCTV may be used for control and management of major events, to ensure that public safety is maintained and to respond quickly to emerging disturbances. An example of this is the large public New Year’s Eve celebrations in the South Australian beachside suburb of Glenelg, where live streamed CCTV monitoring has been used by police for some years. A similar usage is in the active CCTV monitoring of high crime locations or of places such as prisons. In both of these applications, CCTV may be used as a deterrent as well as facilitating rapid response to incidents. Of course this is not always foolproof, as seen in the case of a recent violent melee at Sydney’s domestic airport in which one person died, when

---

<sup>2</sup> A standard 15x10cm photographic print at full resolution requires about 67,500kb. A small web picture or logo will commonly require 16-64kb, and while such an image would be clear at the size of 6x4cm, it would be heavily pixelated at 12x8cm.

<sup>3</sup> A football match would typically be distributed at 1megabit/second for ‘Slow’ connections or 5-12Megabits/second for ‘high-speed’ connections leading to a total of up to 9gb for a one hour broadcast.

<sup>4</sup> Both components and full systems can be purchased online through sites such as Amazon, eBay, or specialist suppliers for less than 1400AUD.

<sup>5</sup> A terabyte is 1,024 gigabytes, while a gigabyte is 1,024 megabytes. Thus a terabyte is equivalent to the storage of 4 to 8 current domestic laptops.

‘despite the banks of CCTV cameras, which are supposedly monitored, it took a member of the public to dial 000 and alert police’ (O’Brien and Creedy, 2009)<sup>6</sup>.

CCTV use in response to crime may involve the deployment of officers in response to an action caught on camera, or provision of specific operational intelligence in real-time support of tactical operations (for example infrared and visible light cameras in a helicopter or unpiloted aerial vehicle). Such operational support video can be used and monitored at the point of capture, however it is frequently sent in real-time (‘as it happens’) to a command and control facility to assist in directing resources. Video captured by police cameras during an operation such as this would normally be retained after viewing as a part of operational record-keeping requirements.

## CCTV EFFECTIVENESS

Our purpose here is to provide a brief overview of this literature, to provide a context to the technical discussion that is the core of our paper. As Wilson and Sutton (2003 p. 1) note, ‘Although CCTV has expanded rapidly in public spaces it remains a controversial measure whose outcomes and appropriateness are hotly contested.’ We follow five key threads in discussing the literature on the law enforcement effectiveness of CCTV: measuring impact; success in preventing crime; accuracy, particularly with regard to convictions; public support and belief in its effectiveness; and workload implications.

Readers of the academic literature on CCTV effectiveness may be struck by the repetition of one particular word: inconclusive. A key reason for this is that it is very difficult to measure impact due to factors such as absence or incompatibility of figures for prior periods, inability to measure whether crime has simply been pushed into other areas, and differing methodologies (see Gill et al., 2007; Gill and Sprigg, 2005; Wilson and Sutton, 2003). Added to this is the challenge of measuring impact, since comparison of crime statistics is fraught by the reality that crime statistics may not be disaggregated to a useful degree, that many factors affect changes in measurements, and that monitoring periods may not be sufficient to draw firm conclusions (Short and Ditton, 1998, p.12; Wilson and Sutton, 2003, p. 2). In this context, Welsh and Farrington (2004) conducted a thorough comparison of a large number of studies to compare the crime deterrent effect of installing CCTV in public spaces with that of increasing lighting. They found that both actions ‘represent effective situational measures for reducing crime’, particularly in the case of property crime (as opposed to violent crime). They also found that in city centres, street lighting had a greater impact on crime than installing CCTV cameras (Welsh and Farrington, 2004, p. 513).

With respect to deterrence, a long term study comparing application of and attitudes to CCTV in eight European countries found that

the majority of CCTV systems aim to prevent deviant behaviour by symbolic but more or less incompetent deterrence because cameras are highly visible but those under surveillance are hardly visible for an observer due to irregular monitoring, informational overkill or even the deployment of dummy cameras. (Hempel and Töpfer 2004, p. 7)

Reinforcing this perspective, Privacy International (2007) notes that the existence of CCTV surveillance in London did not deter the July 2005 terrorist attack, nor did it detect attempted attacks in 2007. In contrast, Gill and Spriggs’ report to the UK Home Office noted that police and security staff found it useful to be ‘able to remind individuals that cameras were watching them as a way of increasing compliance’ (2005, p. 115)

In relation to accuracy, Henderson, Bruce and Burton (2001) conducted a series of tests that revealed that even under optimal conditions, the accuracy of face matching techniques using CCTV, broadcast quality recording, and still photographic images was at best unreliable, not least due to the low quality images used. The highest success rate (75%) for face matching was achieved when comparison was between different posed photographs, while comparing still photographs with CCTV footage of a person achieved a success rate of only 20%. While it has been stated that CCTV footage is particularly useful when ‘you know *who* you are looking for’ (Coleman and Sim, 2000, p. 629, emphasis in original interview), Henderson et al. discovered that even when asked to state which of just two posed photographs showed the offender in a high quality CCTV, accuracy remained at just 65% (2001, p. 460).

There is also some disagreement about the appropriateness of using CCTV for public surveillance. Conflicting social attitudes to these technologies have been reported, both between countries and between social groups (see for example Singer 2009 and Hempel and Töpfer 2004, pp.8-9). Levine (2000) has argued that people’s response to surveillance is significantly influenced by their social location (or ‘group membership’) – that is to say, how they locate themselves in relation to those advocating or performing the surveillance. McCahill and Norris cite a range of papers that report negative effects on young people arising from CCTV usage, whether or not it is specifically targeted at them (2002, p. 14).

---

<sup>6</sup> Such tragic examples are not new, and the Hillsborough football disaster of 1989 stands as a stark example of actively police-monitored CCTV that did not facilitate a police response that saved lives (see McMillan 2009).

Coleman and Sim (2000, p. 635) note that CCTV has been touted as promoting human freedom, in the sense of allowing citizens to feel safe in public spaces, however there has also been protestation that CCTV infringes on people's freedom and privacy. Privacy International (2007) states that the international trend for governments to collect and retain an increasing amount of information about people within their borders implies that 'all citizens, regardless of legal status, are under suspicion.' Mann (1998, p. 94) challenges that the individual has a right to 'self ownership' that is compromised by CCTV, while Vitale (2006, p. 180) writes of a 'creation of a new kind of sociospatial order and a new neoliberal urban subjectivity' – and indeed other authors point to its disproportionate effects on those already marginalised (e.g. White and Sutton, 1995, pp.89-91; Coleman and Sim, 2000, p. 634).

Perhaps the strongest outcomes around CCTV usage can be seen in public perceptions of personal safety, which a range of studies have found to be positive (see Wilson and Sutton, 2003, p. 5, Gill et al., 2007, p. 306). Yet O'Donnell et al. point out that CCTV use 'may be perceived either as promoting the safety of those in the area or as motivated by a lack of trust in the residents' (2009, p.2). In other words, if one feels that surveillance is being used to protect one's person and property, and identifies with the group implementing the surveillance, then one is more likely to feel it is a positive technology. Conversely, however, if one already feels marginalised and mistrusted – as may be the case for example with homeless people, or others who feel they are only liminal members of society – CCTV surveillance is likely to increase this sense/experience of marginalisation.

Finally, in addition to significant physical costs<sup>7</sup>, live streaming of CCTV footage has significant human workload implications. If footage is to be screened live rather than stored, then it must be monitored. Monitoring by police necessarily removes officers from other tasks, at a time when there is continued political and community demand for *visible* policing 'on the streets', and when it is unlikely that policing budgets would be expanded to allow for extra staff to do this work – with the result that some police feel 'imaged out' (Gill and Sprigg, 2005, p. 115). In many cases, CCTV footage is therefore monitored by private groups or individuals, in what Norris and McCahill (2006, p. 105) describe as a move towards 'hybrid policing' in which distinctions between 'public' and 'private' become less clear.

Perhaps the most famous example of this took place in Liverpool Council in the 1990s, when a group of business owners and the city council collaborated to have CCTV cameras installed in key areas of the city, with the intent of increasing perceived safety and thus consumer traffic. While the local police had input into the location of cameras, it was members of the business partnership who undertook monitoring of the camera footage (Vitale, 2006; Coleman and Sim, 2000). A similar example can be found in many Australian cities, where business interests have had input ranging 'from simply offering in principle support through to full responsibility for funding ongoing operations' (Wilson and Sutton, 2003, p.3). In a current example, the Japanese police authority reportedly intends to install security cameras in residential areas in 14 prefectures, and to 'entrust volunteer groups of residents to operate and manage the equipment and image data' (Japan Times, 2009).

Those monitoring or reviewing CCTV footage 'face a daunting task', in that they must make judgements based on limited information (e.g. there is no sound), and in an unnatural context, in which the act of surveillance itself may generate an expectation of guilt (Williams, 2007, p. 100). Michael and Michael (2009, p. 5) argue that the combination of implied guilt and absence of trust can lead to a society in which behaviour is performative, determined by 'what we think we "must" do'. There are also several authors who argue that the expectation of guilt is particularly directed towards marginal groups, and that CCTV is part of a 'process by which economically powerful groups in society gain power through the private management of public space' (Fussey, 2004, p. 231; White and Sutton, 1995).

This brief discussion reveals a range of concerns and opinions regarding CCTV. We identify a gap in this literature concerning the data implications of CCTV, in that we believe that discussion of the utility of CCTV in law enforcement remains incomplete without a full understanding of the various dimensions of the data and monetary costs of CCTV use. We therefore move to that discussion now.

## TECHNOLOGY IMPACT AND IMPLICATIONS

The collection of CCTV video has several impacts on information and communications technology (ICT). These can be loosely categorised as relating to: *volume* (impact on network services and provision of sufficient storage capacity); *integrity* (storage and retrieval and preservation of chain of custody); and *identification* (cataloguing, marking, indexing and searching for data of interest).

Collection of CCTV imagery is not useful in law enforcement unless it is captured and stored in an identifiable manner. The imagery must be of a sufficiently high quality that it can be reasonably expected to accurately and usefully reflect the actions and activities being recorded. The volume of data that is generated by each camera is substantial and must be transferred, stored, marked and labelled, indexed, archived and made available for view or retrieval. The common multi-camera CCTV environment compounds this data transfer and management issue into the kind of problem normally only seen in specialised data processing environments such as video pre-production. For this reason, CCTV

---

<sup>7</sup> For example, the Mayor of Melbourne City Council stated that installing 31 new cameras (to a total of 54) has cost \$AU1.8 million, and maintenance will cost \$AU1 million annually (Johnston, 2009).

data can easily overload an unprepared network in interesting and unexpected ways (as we will explain below) and will quickly overwhelm all but the largest of data storage environments resulting in substantial cost impact.

The expected and supported use of CCTV within an organisation will modify the degree to which CCTV will impact the ICT environment. Decisions such as whether live-feed CCTV footage must be provided to a centralised monitoring facility are critical factors. Optional storage, playback and archive of this data present additional problems. In technical terms, CCTV footage is characterised as large-packet, high-volume, continuous, time-critical, and order-sensitive. Each of these characteristics is important, and in combination they present a uniquely challenging data stream. The high volume of data has some immediately obvious impacts on the underlying network and storage infrastructure. The continuous delivery of large packets also has impacts on both the network and storage infrastructure and on other (seemingly unrelated) applications and services. In other words, communicating this volume of data can cause unexpected problems elsewhere in a system.

### **Diverse scenarios for CCTV networks**

There are several levels of CCTV data communication and storage, with different ramifications for networks and ICT resources and support. We outline three simple CCTV streaming scenarios here as a guide for the reader, to help contextualise the following discussion on ICT implications. In each case, we are talking specifically about *public space* systems, rather than monitoring of private premises. The minimum and simplest case for CCTV use is simply the central collation of CCTV imagery for the purpose of (near) real-time monitoring. This usage case has an impact on network services that, at a base level, is proportional to the number and quality of CCTV cameras in the environment. The lack of a long-term retrieval or review requirement simplifies the data storage needs and almost eliminates any need for a structured data labelling/marketing/indexing and search facility. This environment will experience a reasonably well understood network bandwidth impact. The continuous transfer of CCTV data may also impact other services, such as IP telephony or video conferencing, in a manner that is less obvious.

A somewhat more demanding case involves active monitoring with a medium-term retrieval requirement. This case includes all of the attributes of the previous environment, but also adds a requirement to store CCTV data for longer periods of time. This means that very large volumes of data storage must be provisioned, with a consequent increase in aspects such as: systems/hardware support and maintenance; systems and storage management overhead; data archiving and recovery facilities; physical and environmental factors (space, power, air-conditioning); and the network and licensing costs of maintaining these additional systems.

A much more complex case involves active monitoring with a requirement for strict data integrity, chain of custody protection and search/playback facilities. This environment provides the highest level of data integrity, capacity and capability for review of identified and surrounding footage. This is the hardest and most expensive environment discussed. This environment has the added challenges of requiring multiple and delayed playback facilities; comprehensive audit logging and data tracking capabilities; and an ability to guarantee data integrity.

### **Timeliness**

It is generally expected that, for live-feed CCTV video to be useful in identifying current events, it will be available for display within 2 seconds of capture. CCTV differs from some other video environments (such as video-conferencing) in that the imagery does not need to be transferred with high priority transfer queues to meet very tight time constraints (i.e. instantaneous transmission) and constant frame-refresh rates. The requirement to have the imagery available within 2 seconds does, however, require that all captured data be transferred *as it is collected*, regardless of any other applications or services that the underlying network infrastructure may need to support.

### **Data size**

CCTV system manufacturers regularly recommend video frame-rates of 5 to 15 frames (images) per second, and regularly provide '4CIF' resolution (704x576 pixel) (see for example JSVG, 2009). A single CCTV camera operating at the industry standard 4CIF resolution with H.264 encoding, capturing 10 images per second in a high-traffic public area can easily generate 864,000 frame each day, requiring 6.6 gigabytes (Gb) of data storage and 0.64 Mbps of dedicated network capacity. The same location with a camera collecting digital-TV quality video can easily generate over 200Gb of data per day at a rate of 20 Mbps of constant network traffic for over 1.7 million individual frames. Additionally, an environment using older cameras or less efficient image encoding protocols will get lower quality images with higher data sizes.

The nature of CCTV streaming drives a number of aspects of the transfer of that data over a network infrastructure. Streaming video data manifests as continuous, regular pulses of small groups of large data-packets. This makes it quite different from the majority of traffic that modern data networks are expected to support. The underlying infrastructure and protocols that go together to create a modern data network are designed to ensure the reliable delivery of data (packets) from one system to another. They are designed with the expectation that the arriving data will be reasonably well distributed and fairly random in packet size and frequency. Very few applications have any firm performance requirement, and those few usually have low individual time-on-delivery data volumes (for instance IP telephony, user

authentication, time synchronisation) or have burst-idle traffic flows (database replication, thin-client terminal services). Live streaming of CCTV, however, is both time-critical and high volume and this translates into extremely high pressure on networks.

### **Horizontal impact**

In real terms, as each frame is transmitted (5-20 times per second) the data associated with that frame will be transmitted in a single pulse (burst), each of which will be at least 64kilobits (8kilobytes). This will generate a burst of 4 to 8 maximum size packets in a short continuous stream. This will repeat 5 to 20 times each second. When this traffic exists solely within a single LAN<sup>8</sup>, the impact will be minimal. Where this traffic has to traverse lower-speed networks (such as WAN, Microwave, Satellite or Internet networks) or networks already experiencing some congestion, this pattern of time-critical traffic can have a substantial impact on such resources as WAN/router performance, reliability and quality of IP telephony, backup time, capacity planning, and network management. The impact of these large data packets is further multiplied over legacy or long-distance network connections.

### **Constant Traffic**

An often unexpected impact of real-time streaming video such as CCTV over modern networks is that this workload can cause much greater congestion in small to mid-range network equipment than would normally be expected. Modern networks and protocols are designed to handle relatively random traffic arriving as short, medium- to high-volume bursts, followed by a period of calm. The semi-continuous stream of large data packets that typifies the collection and capture of near-real-time CCTV footage acts to generate a constantly repeating interruption to the 'normal' flow of network operations. The larger and more capable network equipment is designed and built with sufficient local buffering capacity to smooth this localised congestion, and still provide most efficient functioning. Less capable equipment will however suffer local inconsistencies of packet-delay and port congestion that can have a visible impact on the display of real-time streaming video, and a disproportionate impact on time-on-delivery services such as IP telephony. Unlike many streaming video applications, it is not feasible to pre-load live-stream CCTV video.

### **Data Volume**

The storage capacity required to support this volume of data for even a small installation is staggering. As discussed above, a single medium-resolution camera can generate over 6Gb of video per day, 200Gb/month or 2.4Tb per year. An environment such as a small university campus, technology complex or passenger terminal may easily have over 200 cameras. These cameras alone would generate over 128 megabits/second of traffic (enough to fill over 80 home ADSL connections) and need more than 1,300Gb of storage each day. Providing the capacity to store 28 days of this data will require close to 40Tb of disk and/or tape. While the physical dimensions of this storage are roughly equivalent to a bar fridge, it would draw about 4 kilowatts of power<sup>9</sup>, and would need to be maintained in an air-conditioned and environmentally controlled room (with a set-up cost of \$50,000-100,000, and commercial rental costs for the space of around \$3-4,000 per annum).

Network infrastructure faces similar challenges due to both the volume and nature of the traffic. On initial inspection, 0.64 Megabits/second does not appear difficult to modern network professionals who implement networks based on 100 or 1000 Megabit connections for local and/or campus networks. Using the example above, however, the deployment of just 200 cameras requires either the deployment of multiple dedicated 100 Megabit services, or upgrading core networking infrastructure to support 1,000 Megabit solely to service the CCTV management facility.

### **Data Storage**

When contemplating the provision of capacity for storage of CCTV footage, a number of decisions need to be made with respect to how and when the footage will be used, and for how long the footage will be available. Due to the data volume already outlined, many organisations have a hierarchical scheme for maintaining their CCTV footage. For instance, they may by default, keep all cameras for 24 hours, 25% (of-interest cameras) for 48 hours, and 5% (entry/exit cameras) for 7 days. Using the figures described above for 200 standard resolution cameras, this would require: 1.3Tb for the day, 320Gb for of-interest, 330Gb for entry/exit – or about 2Tb purely to support storage of transient CCTV data.

There are several important points to note about this environment. First, it does not provide for storage of ANY video footage beyond seven days, thus any archival or *ad-hoc* storage, labelling, marking or indexing of footage would have to be managed both separately from this system and within those time-frames. Second, this example uses a fairly low resolution environment, such as one that is designed primarily for security guard use, rather than being of use for law enforcement or investigation. Finally, as a point of comparison, 2Tb of storage would constitute a substantial portion of the full corporate data storage resources of many commercial and government environments.

<sup>8</sup> Local Area Network – specifically in this case, a high-speed switched network (100Megabits/second or faster).

<sup>9</sup> An energy efficient office building uses 0.90watts/ft<sup>2</sup> (9.7watts/m<sup>2</sup>), thus 4kw would light over 4000m<sup>2</sup> of commercial office space (California Energy Commission 2008, p.2).

### **Design, operation and audit problems**

The factors outlined above add a layer of complexity in the design, implementation, day-to-day operation of a data environment, as well as in the review and audit processes. This complexity will vary according to the organisation's policies and legislative requirements. These aspects are beyond the scope of the current paper, but warrant further exploration.

## **LAW ENFORCEMENT IMPLICATIONS**

The data volume and impact outlined above constitutes significant implications for any organisation. They are particularly relevant to police forces because CCTV is receiving increasing attention internationally as a point of synergy between emerging technologies, mounting financial constraints on public institutions, and growing demands for visible policing in increasingly risk-averse societies. Indeed, 'the most common reason advanced for installing CCTV in town centres has been to combat loosely defined "anti-social behaviour"' (Wilson and Sutton 2003, p. 2).

Our concern is that installation of these systems places unrealistic expectations on police in terms of ability to resolve crime accurately, as well as unsustainable resource needs that will have significant impacts on other areas of police capacity unless expertly managed. The most recent CCTV systems serve their *intended* purpose very well when installed competently and professionally, with well-defined areas of use. However most such systems are utilised for area surveillance – that is, to provide a general overview of a broad area rather than providing close, sharp images of a face. This renders them close to useless for prosecution in many cases.

The fidelity required for CCTV to be effective in investigation and prosecution has extreme implications for networks and storage. Compounding this, the vast majority are installed by salespeople rather than network specialists, and/or are installed according to budget needs rather than outcome needs, and thus they do not effectively monitor what people think they can monitor. The importance of skilled professional installation of CCTV monitoring systems is critical to deploying a system that can satisfy the implementation objectives without severely impacting on other resources. Critically, these systems cannot be retrofitted to an existing environment, because the technology needs are vastly different.

## **CONCLUSION**

An important question arising from this study is where this information leaves decision-makers within police forces and other organisations. In terms of what is available in the present moment, this information reveals that it is possible to have a very effective monitoring system that is targeted to carefully identified and clearly specified needs. Where this is matched by an appropriately designed system that is professionally installed and fully covered by budget, it will not disrupt other services and may be an effective supplement to other policing measures. Considering these factors carefully before committing to a CCTV system (or any other policing approach) will help to ensure appropriate expectations and operational effectiveness.

In terms of what is desirable, this points to a need to explore ways to a) reduce the raw data network overhead (for instance through improved data compression techniques that don't adversely affect visual acuity); b) enhance the stored data as and when required; and c) improve the point-effectiveness of CCTV through features such as facial recognition technology or facial feature recording. Development is progressing in all of these areas, as is the skill of professional CCTV designers and installation professionals. This means that with time and ongoing technological improvements, CCTV will become an increasingly useful tool in policing. To ensure that this becomes reality, it will be important to have clear communication from police regarding their needs and desires with respect to such systems.

There is not good evidence that CCTV is any more useful in crime prevention than any other ambient factor. For this reason, costs and technological impacts must be carefully considered, and we have shown that these are significant – and certainly not cost-savers for politically and financially pressured law enforcement agencies. Set-up and maintenance costs are further increased when monitoring, data transfer and storage costs are added. For victims of crime, such costs may appear entirely justified if they help to secure convictions, and where clear CCTV images exist, investigators and prosecutors will find their tasks more streamlined and efficient.

In contrast, low image quality, conflicting goals of camera systems (e.g. area surveillance vs. face identification), and inadequate ICT systems can severely undermine the utility of CCTV in crime prevention. In this sense, CCTV systems must be carefully planned: systems aimed at deterrence or perhaps rapid response to incidents at events such as sporting matches require significantly less storage capacity, lower image quality and thus less streaming capacity. It should not be expected, however, that such a system would be equally effective for prosecution. On this basis, it is important to fully understand technological implications as well as effectiveness of CCTV *before* systems are designed, costed and implemented.

CCTV is not a golden bullet: it requires significant financial, technological, storage and systems input to work effectively – and even then, challenges remain such as the social impacts on marginalised groups. We conclude that

police (and their governments) would be well advised seriously to consider alternative means of meeting identified needs before turning to CCTV. The kind of investment needed for CCTV that fulfils the fourfold law enforcement purpose (deterrence, rapid response, investigation and identification, and prosecution of crime) is certainly not a cost- or resource-saving exercise. Video-based surveillance systems are surprisingly resource-intensive, expensive and task-specific.

## REFERENCES

- AAP. (2007). *Hundreds of CCTV cameras for APEC*, July 8 2007. Retrieved August 22 2009, from [www.news.com.au/story/0,,22037971-1242,00.html](http://www.news.com.au/story/0,,22037971-1242,00.html).
- California Energy Commission. (2008). Task/Ambient Lighting: Efficient, Stylish, and portable, *PIER technical Brief*. Retrieved November 22 2009, from [www.energy.ca.gov/research](http://www.energy.ca.gov/research).
- Coleman, Roy and Joe Sim. (2000). "You'll Never Walk Alone": CCTV surveillance, order and neo-liberal rule in Liverpool city centre, *British Journal of Sociology* 51(4), 625-639.
- Fussey, Pete. (2004). An interrupted transmission? Processes of CCTV implementation and the impact of human agency, *Surveillance and Society* 4(3), 229-256.
- Gill, Martin, Jane Bryan and Jenna Allen. (2007). 'Public Perceptions of CCTV in Residential Areas: "It Is Not As Good As We Thought It Would Be"', *International Criminal Justice Review* 17(4), 304-324
- Gill, Martin and Angela Spriggs. (2005). Assessing the impact of CCTV, *Home Office Research Study 292*, United Kingdom: Home Office Research, Development and Statistics Directorate.
- Hempel, Leon and Eric Töpfer. (2004). CCTV in Europe: Final report, *Working Paper No.15*, Berlin: Centre for Technology and Society, Technical University Berlin.
- Henderson, Zoe, Vicki Bruce and A. Mike Burton. (2001). Matching the faces of Robbers Captured on Video, *Applied Cognitive Psychology* 15, 445-464.
- Japan Times. (2009) Security Camera Networks Eyed: Residential streets to get cop cameras, *Japan Times* June 26 2009. Retrieved July 8 2009 from [www.japantimes.co.jp](http://www.japantimes.co.jp).
- Johnston, Matt. (2009). Melbourne Mayor Robert Doyle ready for more CCTV cameras, *Herald Sun* August 20 2009. Retrieved August 22 2009 from [www.news.com.au/heraldsun/story/0,,25957996-5000117,00.html](http://www.news.com.au/heraldsun/story/0,,25957996-5000117,00.html).
- JSVG. (2009). *Bandwith Storage Space Calculation*. Retrieved August 15 2009 from [www.jvsg.com/bandwidth-storage-space-calculation](http://www.jvsg.com/bandwidth-storage-space-calculation).
- Levine, M. (2000). SIDE and Closed Circuit Television (CCTV): Exploring surveillance in a public space, in T Postmes, R Spears, M Lea, S Reicher (eds.), *Side issues Centre Stage: Recent development in studies of de-individualisation in groups*. Amsterdam: Royal Netherlands Academy of Arts and Sciences.
- Mann, Steve. (1998). "Reflectionism" and "Diffusionism": New tactics for deconstructing the video surveillance superhighway, *Leonardo* 31(2), 93-102.
- Martin, Chris. (2009). Freedom's fine line as cops go on the wire, *The Australian* July 11 2009. Retrieved August 22 2009 from [www.theaustralian.news.com.au/story/0,,25761048-28737,00.html](http://www.theaustralian.news.com.au/story/0,,25761048-28737,00.html).
- McCahill, Michael and Clive Norris. (2002). Literature Review. *Working Paper no. 2*, University of Hull: Centre for Criminology and Criminal Justice. Retrieved August 22 2009 from Available at [www.urbaneye.net/results/ue\\_wp2.pdf](http://www.urbaneye.net/results/ue_wp2.pdf).
- McMillan, Nicola. (2009) *The Hillsborough Football Disaster: Context and Consequences*, Great Britain: Em-Project Limited.
- Michael, M.G. and K. Michael. (2009). Uberveillance: Microchipping People and the Assault on Privacy, *Quadrant* LIII(3), 85-89.
- McCahill. (2006). CCTV: Beyond Penal Modernism?, *British Journal of Criminology* 46, 97-118.
- O'Brien, Natalie and Steve Creedy. (2009) Sydney Airport in the dark on bkie threat, *The Australian*, March 24 2009. Retrieved August 22 2009 from [www.theaustralian.news.com.au/business/story/0,,25232851-23349,00.html](http://www.theaustralian.news.com.au/business/story/0,,25232851-23349,00.html).
- O'Donnell, Aisling T, Jolanda Jetten and Michelle K Ryan. (2009). Who is Watching Over You? The role of shared identity in perceptions of surveillance, *European Journal of Social Psychology*, published online. Retrieved July 8 2009 from [www.interscience.wiley.com](http://www.interscience.wiley.com).

- Privacy International. (2007). *Video Surveillance*, December 18 2007. Retrieved August 22 2009 from [www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559088#\[51\]](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559088#[51]).
- Short, Emma and Jason Ditton. (1998). Seen and now heard: Talking to the targets of open street CCTV, *British Journal of Criminology*, 38(3), 404-429.
- Singer, Jill. (2009). Bring on City's Big Brother, *Herald Sun* August 21, 2009. Retrieved August 22 2009 from [www.news.com.au/heraldsun/story/0,,25957996-5000117,00.html](http://www.news.com.au/heraldsun/story/0,,25957996-5000117,00.html).
- Vitale, Alex. S. (2006). Review, *Contemporary Sociology* 35(2), 179-181.
- Welsh, Brandon C and David P Farrington. (2004). Surveillance for Crime Prevention in Public Space: Results and policy choices in Britain and America, 3(3), 497-526.
- White, Rob and Adam Sutton. (1995). Crime prevention, urban space and social exclusion, *Journal of Sociology* 31(1), 82-99.
- Williams, David. (2007). Effective CCTV and the Challenge of Constructing Legitimate Suspicion Using Remote Visual Images, *Journal of Investigative Psychology and Offender Profiling* 4, 97-107.
- Wilson, Dean and Adam Sutton. (2003) Open-Street CCTV in Australia, *Trends and Issues in Crime and Criminal Justice No. 271*. Canberra: Australian Institute of Criminology.

## **COPYRIGHT**

Vandra Harris & Crispin Harris ©2009. The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors

# Security Decay: An entropic approach to definition and understanding

Michael Coole<sup>1</sup> & David J. Brooks<sup>2</sup>

<sup>1</sup>Western Australian Department of Corrective Services (DOCS)

<sup>2</sup>Security Research Centre (SECAU)  
Edith Cowan University

## Abstract

*This article discusses the affect decay has within a systems approach used when implementing security strategies, in particular, the theory of defence in depth. Defence in depth is implemented within a risk management framework to reduce an organisation's identified risks, which could lead to undesirable and unacceptable consequences. Defence in depth aims to link layered security elements into a system to ensure a holistic and functional security system, underpinned by the functions of; deter, detect, delay, response and recovery. For such a system to be commissioned and maintain its commissioning effectiveness, these functions must be performed in their sequential order and within a period of time, which is less than an adversary's attack time.*

*This paper argues that such a relationship between the defence in depth elements requires an orderly relationship and that factors which impede this orderliness, directly affects the security system as a whole. A method to understand such deterioration of orderliness is the concept of entropy, referred to as the steady degradation of a system. Underpinned by the characteristics of disorganisation and decay, a security system can become degraded through the reduction in effectiveness of its individual components. Such degradation reduces the effectiveness of the whole system, considered in this paper as entropic security decay. Within the risk management framework, it can be argued that as security decay increases, risk reduction decreases and therefore, risk exposure increases.*

## Keywords

Security, decay, entropic, defence-in-depth, risk management

## INTRODUCTION

The concept of risk management is well established in academic and organisational literature and to some degree, so is security risk management; however, the effectiveness of security risk management has been questioned (Brooks, 2009). Therefore, this paper discusses how security risk management may be implemented in a systems approach, using the theory of defence in depth whilst considering the concept of entropy. It has been proposed that defence in depth strategies can be impeded by the characteristics of disorganization and decay underpinning this concept. For an organisation to maintain a sound security profile, all defence in depth elements and their constituents must be maintained at their optimum level of performance. It is argued that security science should draw on the concept of entropy to establish the concept of security decay. Security decay results in a reduction in overall system performance, which should be avoided through the active monitoring and reviewing of treatment strategies.

## STUDY OBJECTIVES

The objectives of this paper were to provide a framework that developed the term *entropic security decay*, providing a definition for security decay, establishing where security decay integrates into the security risk management cycle and stimulate academic discourse into the concept of security decay.

## BACKGROUND OF THE STUDY

In contemporary business, risk management is considered a significant management activity. Borgsdorf and Pliszka (1999, p. 6) define it as "the planning, organising, leading and controlling of an organisation's resources" to minimise the potential of negative effects on the business activity. This approach is a formal systematic process (Hatfield & Hipel, 2002, p. 1054) that is supported through Australian Standards in risk management (Standards Australia, 2004) and security risk management (Standards Australia, 2006).

The risk management concept has been embraced by security management for planning how organisational resources can be efficiently and effectively managed to reduce the chances of negative outcomes from breaches of security programs (Broder, 2006, p. 25). Such a planning process in security management is, in general, referred to as *security risk management*. In addressing risk concerns, Standards Australia HB167 Security Risk Management (2006, p. 63) state that the key elements of organisational, community or individual security controls are those components which

contribute to the management of risks through their ability to deter, detect, delay, respond and recover from attacks. Therefore, a security risk management plan determines the level of treatment controls required, based on a facility's risk rating and are implemented in accordance with the theory of defence in depth (Garcia, 2001).

## SIGNIFICANCE OF THE STUDY

The security industry, both government and commercial, rely on the application of security risk management. Security risk management is unique from other forms of risk management, where many of the more generic risk models lack key concepts necessary for effective design, application and risk mitigation (Brooks, 2009, p. 1). Nevertheless, within the context of security risk management it is expected that characteristics that may make an organisation more prone to entropic security decay can be identified and measured. Once these characteristics are understood, this will allow the use of stimulus funding to maintain the effectiveness of various security risk mitigation strategies.

## DEFENCE IN DEPTH

Security, as a discipline, collectively embraces a historically consistent strategy towards preventing theft, destruction of facilities, the protection of personnel and information, referred to as *defence in depth*. As such, the underlying theory for this study was defence in depth, comprising of various elements such as *deterrence, detection, delay, response* and *recovery*. This strategy has been applied to the protection of assets for centuries, based on the argument that a protected asset should be enclosed by a succession of barriers that restricts penetration of unauthorised access to provide time for an appropriate response (Smith, 2003, p. 8) and to facilitate recovery.

The theory of defence in depth aims to link layered security elements into a system incorporating; people, technology, barriers and procedures, to ensure a holistic and functional security system (Smith, 2003, p. 8). This system delivers effective risk based decisions, enhanced operational effectiveness and a reduction in overall risks and costs (Trusted Information Sharing Network, 2008, p. 2).

Defence in depth is employed in security risk management using a systems approach (Garcia, 2001, p. 6), based on a cost benefit analysis framework (Manunta, 2007). A system can be defined as an "integrated collection of components or elements designed to achieve an objective according to plan" (Garcia, 2001, p. 6). Fennelly (1997, p. 59) supports a systems approach to security arguing that maximum security is a concept, whereas alarm systems, physical barriers, guard forces and other components of a security system do not individually achieve security. Therefore, a systems approach includes the component resources of people, techniques, procedures, design features, materials and educational programs integrated to construct a security program (Post, Kingsbury & Schachtsiek, 1991, p. 23). The combination of such resources may be integrated to form a physical protection system.

The objective of a physical protection system (PPS) is to eliminate accomplishment of a malevolent overt or covert action, preventing sabotage of critical equipment, theft of assets or information and the protection of people. In line with the theory of defence in depth, for a PPS to meet these objectives there must be an awareness that an attack is underway (detection), the slowing of an adversary's progress to the target (delay) and enough time for the response force to interrupt or stop the adversaries (response) before they achieve their goal (Figure 1).

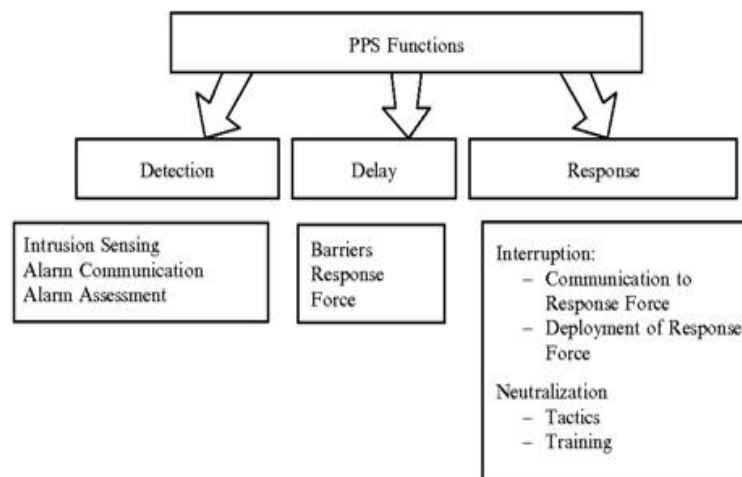


Figure 1 Functions of a physical protection system

(Garcia, 2006, p. 34)

**Relationship of physical protection system functions**

The interrelationships between the functions of the PPS commence with the element of detection, which begins on receipt of the first alarm and concludes with accurate assessment. The delay function must slow-down an adversary to allow a response force enough time to deploy and interject the adversary. This delay time must be less than the adversary's task or attack time, which is the total time required for the adversary to accomplish their desired goal (Figure 2).

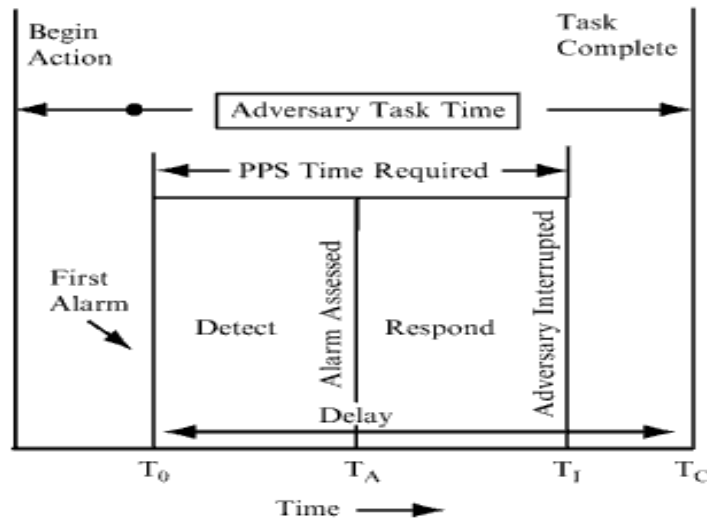


Figure 2 Interrelationships of physical protection system functions

(Garcia, 2006, p. 39)

For example, a sensor first activates at time  $T_0$ , but the time when the alarm is assessed as valid is  $T_A$ . From these points in time, the location of the alarm must be communicated to the response force. The time at which the response force interrupts the adversary is labelled  $T_I$  and the adversary task completion time is  $T_C$ . For a PPS to accomplish its objective of interrupting an adversary,  $T_I$  must occur before  $T_C$ . In addition, detection should occur as early as possible and  $T_0$ ,  $T_A$  and  $T_I$  should be as far to the left on the time axis as possible (Garcia, 2006, pp. 37-38).

**AN ENTROPIC APPROACH TO DEFENCE IN DEPTH**

Defence in depth has historically shown its effectiveness for security concerns (Smith, 2003, p. 8); however, King (2008, p. 1) warns such security controls inevitably degrades over time. Such degradation results in a security system suffering from natural entropy. The concept of entropy is derived from a physics metric, defined as a measure of disorder in a system and a process characterised with decay, disintegration, running down and disorder (Bohm & Peat, 2000, p. 137; Herman, 1999, p. 86). Such system degradation reduces efficiency and effectiveness (Bohm & Peat, 2000, p. 137). According to Callister (1997, p. 482) entropy increases with increasing disorder; however, the concept of entropy is a tremendously difficult physics concept to grasp when considering disorganisation and decay in various types of systems (Lovey & Manohar, 2007, p. 99; Styer, 2000, p. 1).

Herman (1999, p. 86) broadly defines entropy as the steady degradation of a system — where entropy increases within a system, capability decreases — based on the argument that systems rely on order and cohesion. The laws of physics states disorder must always increase, as in classical physics the laws of nature are perfectly time-reversible, where all of the processes people see occurring do so in one direction only. Reversal would go against the laws of statistical probabilities, referred to as the second law of thermodynamics (Felder, 2001, p. 1). Total entropy of the universe can never decrease, as according to Lovey and Manohar (2007, p. 99) this law states that transformations of one form of energy into another in natural process is accompanied by a loss because of increasing entropy. The science of thermodynamics enables the quantity known as entropy to be measured objectively in terms of the amount of heat and work that is associated with a system, as left to itself a physical system tends to maximise its entropy in-line with the laws of thermodynamics (Lovey & Manohar, 2007, p. 99; Styer, 2000, p. 1).

$$\text{System effectiveness} = \frac{\text{capability}}{\text{entropy}}$$

Maximum entropy is associated with a systems inability to carry out work, transfer useful energy from one region to another or in any other way, and generate global orders of activity. Motz and Weaver (1989, p. 168) suggests that all systems strive towards disorder, which when achieved the system will be in a state of equilibrium. Complete equilibrium in a system results in the death of the system.

## SECURITY SYSTEM ENTROPIC DECAY

A security system is only as good as its parts; when a single part fails, this failure can cause degradation within the total system (Konicek & Little, 1997, p. 184; King, 2008, p. 1). Garcia (2006) concurs, suggesting that system effectiveness can become degraded through the reduction in effectiveness of individual components.

As such, this paper has used the concept of entropy to discuss the decaying effects on a physical protection system (PPS), in-line with King's (2008, p. 1) assertion that security systems inevitably degrade over time due to natural entropy. However, according to Denbigh (2009, p. 4) for entropy to have an effect on a system it must have initially been considered orderly, where orderliness is capable of being quantitatively stated. For a system to be defined as orderly, it's elements must be appropriately distributed in space and/or time, where the rule of orderliness states that a set of three or more objects will display a certain orderliness if they exist in a linear arrangement, for example objects A, B and C. In this context, the objects obey the rule as B is to the right of A, and C is to the right of B, etc. In addition, the same objects will display the kind of orderliness if a relationship also exists between successive separations AB, BC, AC, etc., resulting in a more comprehensive state of order.

It is argued that entropy relates to a security system as the defence in depth functions must be performed in their sequential order and within a period of time, which is less than the time required for the adversary to complete their task (Garcia, 2001, p. 6). These functional requirements of defence in depth are distributed in space and/or time according to Denbigh's (2009, p. 4) entropy rule. The available literature indicates that the space and time distribution of the defence in depth elements create a comprehensive state of order in relation to a PPS macro level of effectiveness. The micro states within defence in depth include the constituents within the elements of deter, detect, delay, and response, which may be considered a linear arrangement (Denbigh, 2009, p. 4; Garcia, 2001, p. 6). Deterrence (element A) is linear to detection (element B), which is linear to delay (element C) followed by a linear response (element D), nevertheless, linearity does not confer equality.

Orderliness also exists within a PPS (Denbigh, 2009, p. 4) for example, deterrence. Deterrence is achieved by altering the cost benefit analysis of a rational choosing adversary (Singh, 2005). Within a PPS each function of the defence in depth strategy within this linear relationship must be achieved in their sequential order, achieving deterrence through systematic application of detect, delay, response (Garcia, 2006, p. 240) and recovery, in this sequential combination. This systematic combination aims to communicate to potential adversaries that the risks outweigh the benefits, influencing their (however rudimentary) cost benefit equation (Clarke & Cornish, 1987, p. 934). Deterrence is related to an adversary's chances of being detected (B), the difficulty in achieving their goal (C), and the chances of getting caught (D). Therefore, deterrence has an orderly relationship with all other elements within a PPS, being D\*BCD.

Another orderliness relationship exists between response (D) and detection (B). Response is an organisation's means of interrupting an adversary before they achieve their goal; however, for response to be achieved there must be knowledge that an attack is underway (detection). Therefore a relationship exists between response and detection, namely D\*B. Further, delay is the means by which the facility provides their response force with enough time to interrupt an adversary. Therefore, delay has an additional kind of orderly relationship with response, C\*D.

In addition, each element of defence in depth has a vertical relationship with its constituents, which combined provides the specific capability for that element within the linear relationship. For the system of defence in depth to be effective, the relationships between the constituents and elements must be orderly and each constituent must be at its desired level of effectiveness.

This paper argues that the macro state of the defence in depth system is recognised as an expression of the average of the microstate variables collectively, where changes in microstates (defence in depth constituent elements) directly affect the macro state. Such a process is based on the definition of entropy offered by Bohm and Peat (2000, p. 137), where disorder within and between elements increases, decay increases and capability decreases.

## ENTROPIC SECURITY DECAY DEFINED

Entropy can be quantitatively stated for defence in depth, using its traditional effectiveness measure. The effectiveness measure of a physical protection system (PPS) is the principle of timely detection; therefore, the macro-state of a PPS

can be represented as its probability of interruption ( $P_i$ ).  $P_i$  is the probability of interruption or the cumulative probability of detection where there is enough time remaining for the response force to interrupt the adversaries. For a PPS, the higher the probability of interruption ( $P_i$ ) the lower the chances of a successful penetration; whereas, the lower the  $P_i$  the higher the chances of penetration (Garcia, 2001, p. 246). The PPS can be analysed using the EASI model (Garcia, 2001), where input parameters representing the PPS functions of detection, delay and response are required. This model demonstrates the relationship among the performance measures of the PPS constituents, represented by the following input parameters:

- $P_s$  = probability that individual detection constituents will sense abnormal or unauthorised activities;
- $P_d$  = the product of the probability that the detection constituents will sense abnormal or unauthorised activities,  $P_d$  represents the element of detection;
- $P_t$  = the probability that the alarm indication will be transmitted to an evaluation or assessment point;
- $P_a$  = the probability of accurate assessment;
- $P_c$  = probability of guard communication;
- Mean and standard deviation of delay time;
- Mean and standard deviation of response time.

These measures are the cumulative sum of the various subsystems within a PPS, where any changes in these inputs have an overall effect on the output (probability of interruption). Therefore, changes in the microstates have a direct effect on the macrostate of the PPS. For example, the small effects in the microstates when calculating the probability of interruption using EASI adversary path analysis (Table 1).

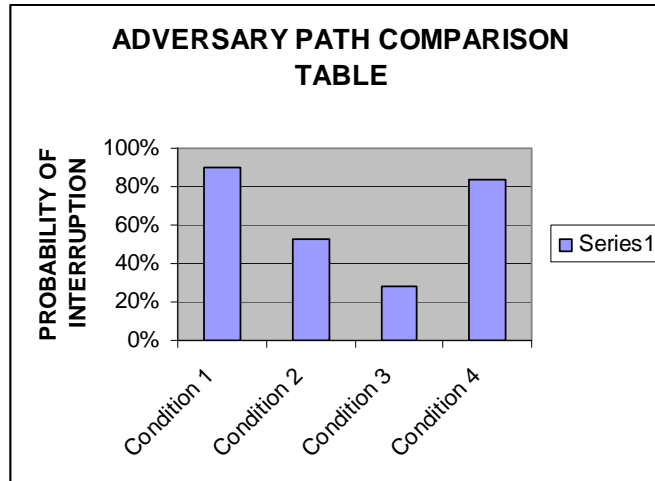


Table 1 Adversary path comparison

Condition 1 (Table 1) indicates a  $P_i$  of 90% (very high chance of interruption) after entering the microstate data. However, condition 2 indicates a much lower  $P_i$  after making small changes in the system’s microstates, as a result of a detection sensors reduced effectiveness due to decay resulting in a higher nuisance alarm rate and by slight increases in response time due to decay in the facilities response capability. Condition 2 (Table 2) indicates a  $P_i$  of just 53% (medium chance of interruption).

Condition	$P_D$	$P_D$	$P_D$	$P_{comms}$	Mdelay (secs)	Mdelay SD (secs)	Mrespond (sec)	Mrespond SD (sec)
1	0.9	0.9	0.9	0.95	332	99.6	200	60.0
2	0.5	0.9	0.9	0.95	332	99.6	300	90.0
3	0.5	0.9	0.9	0.50	332	99.6	300	99.6
4	0.9	0.9	0.9	0.95	452	135.6	300	90.0

Table 2 Physical protection system microstate data

Condition 3 (Table 1) indicates how the probability of interruption can be further reduced with a change in the facility’s probability of communication due to decay in the communications system. This condition shows  $P_i$  of just 28% (Table 2); however, with small changes in the systems microstates through correcting the detection fault, slightly increasing the facility’s mean delay time and correcting the communication systems degradation, condition 4 shows (Table 1) an increased  $P_i$  of 84% (high chance of interruption) after entering the microstate data (Table 2). These examples demonstrate that the systems constituents have a direct influence on its  $P_i$  (macrostate), establishing a time penetration continuum.

The concept of entropy is becoming increasingly popular and used to discuss the state of various systems, including information security systems (King, 2008), organisational systems (Lovey & Nadkarni, 2007) and combat systems (Herman, 1999). However, the meaning of entropy is difficult to define and not well understood outside of academic circles, leading to ubiquitous usage and minimal general understanding. Whilst various definitions and understandings are applied to entropy, a central theme is how various components of a system relate to one another towards producing a coherent whole.

As such, this paper has argued that the concept of entropy provides a framework towards measuring the gradual degradation of a physical protection system after it’s commissioning, reducing its effectiveness. However, given the ubiquitous usage of entropy, limited understanding and definitional ambiguity, this paper argues that the term *security decay* become adopted to represent the measure of degradation within a PPS. The adoption of *security decay* will provide functional definition and therefore, appeal to both security academics and practitioners alike. The paper has proposed that security decay be defined as:

The gradual degradation of the microscopic quantities (constituents), or the gradual degradation in the relationship between the microscopic and macroscopic quantities within a security system.

Such a definition provides rigour and genuine conceptual substance that can be integrated into a physical protection systems performance measure. In addition, such an approach may also be applied to personnel and information security frameworks to encompass the security management functions.

## ENTROPIC SECURITY DECAY AND SECURITY RISK MANAGEMENT

In general, security risk management is considered an important aspect in the function of security management. Why, how and where resources may be directed is often informed by security risk management (Brooks, 2009). Therefore, the concept of security decay has to be embedded within security risk management. As Lovey and Manohar (2007, p. 99) suggest, various systems suffer from entropy and therefore, organisations must understand that for a system to operate efficiently they must continually invest in resources to maintain system adequacy to reduce natural entropy. King (2008, p. 1) supported this view, stating that it is the gradual erosion of seemingly minor security controls that eventually lead to major incidents. As such, the security risk management cycle has to, in some form, incorporate the decaying of risk reduction strategies (Figure 3).

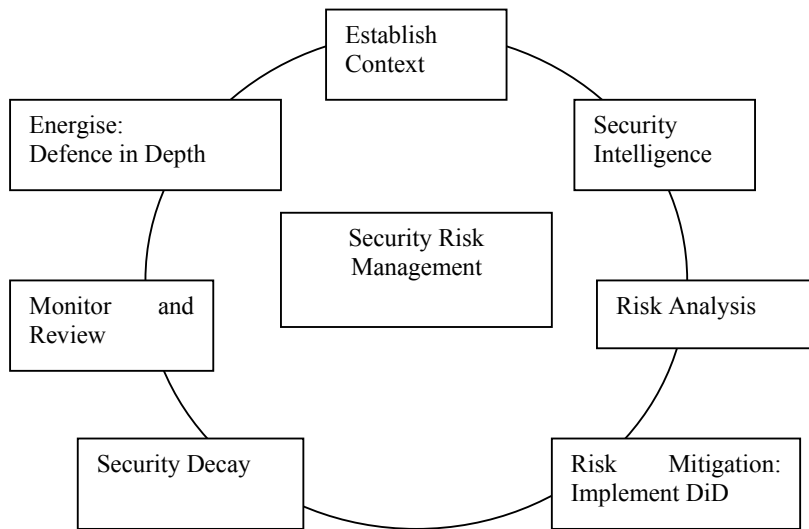


Figure 3 Security risk management cycle, with security decay

(Adjusted from the Trusted Information Sharing Network, 2008, p. 4)

In essence, the security risk management cycle (Figure 3) may have the component of security decay in-built, through the *Monitor and Review* process; however, there are discrete benefits in understanding security decay as a discrete function. Whilst the concept of security decay has been considered by Underwood (1984) and McClure (1997), there is a dearth of knowledge relating to the gradual degradation of security controls. The concept of security decay is an area suitable for continued development and research, a view put forward by this paper is that the concept of entropic security decay becomes adopted by both industry and academia. In addition, the study recommends future research to be undertaken towards establishing support for the concept entropic security decay, focusing on quantitatively defining entropic decay characteristics within the physical protection system, and developing organisational measures and indicators.

## CONCLUSION

This paper has used the physics metric known as entropy to explain how various systems, including security systems, can be reduced in their efficiency and effectiveness when they, their component elements, or constituents become disordered, run-down, degraded or decayed. Entropy is associated with a system's inability to carry out work, transfer useful energy or maintain orders of activity, and all systems strive towards disorder that when achieved, are in a state of equilibrium or death.

In considering defence in depth, the concept of *entropic security decay* has been presented. Defence in depth is the sum of various elements, namely deterrence, detection, delay, response and recovery. The concept of entropy supported the argument that any change in the efficiency and effectiveness of any of the defence in depth elements reduces the system's effectiveness. The sum of these concepts collectively form and were referred to as *security decay*, being defined as the gradual degradation of the microscopic quantities (constituents) or the gradual degradation in the relationship between the microscopic and macroscopic quantities within a security system.

## REFERENCES

- Borgsdorf, D., & Pliszka, D. (1999). Management your risk or risk your management. *Public Management*, 81(11), 6-10.
- Broder, J. F. (2006). *Risk analysis and the security survey* (3rd ed.). Oxford: Butterworth-Heinemann.
- Brooks, D. J. (2009). *Key concepts in security risk management*. Saabruken: VDM Verlag.
- Bohm, D., & Peat, D. (2000). *Science, order, and creativity* (2nd ed.). New York: Routledge.
- Callister, W. D. (1997). *Materials science and engineering: An introduction* (4th ed.). New York: John Wiley & Sons.
- Clarke, R. V., & Cornish, D. B. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, 50(4), 933-947.
- Denbigh, K. G. (2009). *Note on entropy, disorder and disorganization*. Retrieved April 2009 from <http://www.endeav.org/evolut/text/denbig1/denbig1e.htm>
- Edith Cowan University, (2004). *Physical security: Study guide SCY 1101*. Perth: Author.
- Felder, G. (2001). *Things fall apart: An introduction to entropy*. Retrieved April 2009 from <http://www4.ncsu.edu/unity/lockers/users/f/felder/public/kenny/papers/entropy.html>
- Fennelly, I. J. (1997). *Effective physical security* (2ne ed.). Amsterdam; Boston. Butterworth-Heinemann.
- Garcia, M. L. (2001). *The design and evaluation of physical protection systems*. Boston: Butterworth Heinemann.
- Garcia, M. L. (2006). *Vulnerability assessment of physical protection systems*. Boston: Butterworth-Heinemann.
- Hatfield, A. J., & Hipel, K. W. (2002). Risk and systems theory. *Risk Analysis*, 22(6), 1043-1057.
- Herman, M. (1999). *Entropy based warfare: Modelling the revolution in military affairs*. Retrieved April 2009 from <http://209.85.173.132/search?q=cache:7Rigu4CTvaAJ:www.au.af.mil/au/awc/awcgate/jfq/1620.pdf+herman+entropy+based+warfare&cd=1&hl=en&ct=clnk&gl=au>
- King, S. (2008). Computer weekly. Retrieved April 2009 from [http://www.computerweekly.com/blogs/stuart\\_king/2008/09/security-entropy.html](http://www.computerweekly.com/blogs/stuart_king/2008/09/security-entropy.html)
- Konicek, J., & Little, K. (1997). *Security, ID systems and locks: The book on electronic access control*. New York: Butterworth-Heinemann.
- Lovey, I., & Nadkarni, M., S. (2007). *How healthy is your organisation*. Westport, Connecticut: Praeger Publishing.
- Manunta, G. (2007). The management of security: How robust is the justification process? *Security Journal*, 20, 41-43.
- McClure, S. A. (1997). *Security decay: The erosion of effective security*. Unpublished honours thesis, Edith Cowan University, Perth, Western Australia.
- Motz, L., & Weaver, J. H. (1989). *The story of physics*. New York: Plenum Press.
- Post, R. S., Kingsbury, A. A., & Schachtsick, D. A. (1991). *Security administration: An introduction to the protective services* (4th ed.). Boston: Butterworth-Heinemann.
- Singh, A. M. (2005). Private security and crime control. *Theoretical Criminology*, 9, 153-174.
- Smith, C. L. (2003). *Understanding concepts in the defence in depth strategy*, School of Engineering and Mathematics. Edith Cowan University, Perth, Western Australia.
- Smith, S. (1992). Global dumbing: the politics of entropy. *Progressive Review*. Retrieved April 2009 from <http://prorev.com/dumbing.htm>
- Standards Australia. (2004). *AS/NZS4360:2004 Risk management*. Sydney: Standards Australia.
- Standards Australia. (2006). *Security risk management*. Sydney: Standards Australia.

Styer, D. F. (2000). Insight into entropy. *American Journal of Physics*, 68(12), 1090-1096.

Trusted Information Sharing Network for Critical infrastructure Protection, (2008). *Defence in depth*. Retrieved April 2009 from [http://www.dbcde.gov.au/\\_data/assets/pdf\\_file/0006/88359/Defence-in-Depth-CIO-15\\_Oct-2008.pdf](http://www.dbcde.gov.au/_data/assets/pdf_file/0006/88359/Defence-in-Depth-CIO-15_Oct-2008.pdf)

Underwood, G. (1984). *The security of buildings*. London: Butterworths.

## **COPYRIGHT**

Michael Coole & David J. Brooks © 2009. The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

## Professional Intelligence Judgement Artistry: Some early observations

Jeff Corkill  
School of Computer and Security Science  
Edith Cowan University

### Abstract

Intelligence analysis is critical national security and law enforcement function dependant on the intellectual capacity of individual analysts. The practice of intelligence is undertaken in an extremely complex environment often under a veil of secrecy, and where uncertain and deceptive information represents the norm. In order to develop as a profession appropriate constructs with which to explore and explain how analysts process intelligence, make decisions and reach judgements are needed. An improved understanding will offer opportunities to develop appropriate training and professional development for intelligence analysts. This paper introduces the construct of Professional Intelligence Judgement Artistry together with some very early findings to emerge from an initial series of interviews undertaken as part of a pilot study.

### Keywords

Intelligence, analysis, professional artistry

### INTRODUCTION

In the post 9/11 environment a rich body of knowledge has emerged as scholars from within and external to the intelligence profession have sought to define what intelligence is and what it is that intelligence analysts do (Cooper, 2005; George, 2004; Johnston, 2005; Lefebvre, 2004; Marrin, 2009; Marrin & Clemente, 2005; Russell, 2004). That body of literature has further grown as the intelligence community sought to understand why intelligence fails, what constitutes good analysis, the relationship between analysts, agencies and decision-makers and what represents analytical best practice (Cooper, 2005; Moore, Kirzan, & Moore, 2005; Swenson, 2003). Intelligence analysis is very much a human practice very much dependant on the intellectual capacity of individual analysts. Moreover the practice of intelligence is undertaken in an extremely complex environment often under a veil of secrecy, and where uncertain and deceptive information represents the norm. In order to develop as a profession appropriate constructs with which to explore and explain how analysts process intelligence, make decisions and reach judgements are needed. An improved understanding will offer opportunities to develop appropriate training and professional development for intelligence analysts. This paper introduces the construct of Professional Intelligence Judgement Artistry together with some very early findings to emerge from an initial series of interviews undertaken as part of a pilot study.

### Background & Significance

The use of intelligence is not limited to national security and defence domains. Intelligence plays a significant factor in the compliance and enforcement roles of governments (Gill & Phythian, 2006). Intelligence is recognised as a key function of modern law enforcement as it enhances law enforcement effort. The perceived value of intelligence in law enforcement is demonstrated in the common use of the term 'intelligence led policing' in various parts of the world (Cope, 2004; Grieve, 2004, p. 25; Ratcliffe, 2004, p. 5).

Whilst the popular media characterizes intelligence as consisting of such things as spies and secret collection technology, the critical element of successful intelligence production is, and remains the intelligence analyst. This proposition is demonstrated by the fact that it is the analyst who initiates collection of information, and who processes, integrates and interprets that information. It is argued that it is the analyst who creates and disseminates intelligence products, generates context and provides insights all necessary for optimal decision making (Cooper, 2005; Lefebvre, 2004; Rieber, 2004). To date there has been very little research into the role of the law enforcement analyst. This research therefore will contribute to the body of knowledge by providing understanding of what constitutes the difference between average and outstanding law enforcement intelligence analysts.

### Professional Artistry

Schon (1992) first introduced the concept of *professional artistry* as a construct that could explain the higher level competence of skilled professionals working in the murky complexity of real world problems where theory did not always provide the appropriate answer. Subsequently scholars across a range of disciplines have adapted and utilised the concept of professional artistry to formulate constructs in which to examine higher level competence in real world professional scenarios across a range of disciplines including education, health and management (Grainger, 2003; Paterson, 2003; Sadler-Smith & Smith, 2006). Paterson(2003) posited the construct *Professional Practice Judgment Artistry* as means of explaining the complexity of judgement and practice as it pertains to the domain of occupational therapy. Professional intelligence analysts are required to make complex judgments at the micro, macro and meta-levels that optimise decision making on the part of the client for particular circumstances and within a specific context

in a similar way to Paterson’s occupational therapists. Analogous to Paterson’s model, intelligence analysts process complex problems including moral and ethical issues, which may question values, beliefs and assumptions; the outcomes of which may impact on a specific individual through to national security scenarios that impact the entire community. On that basis it does appear that the concept of *professional artistry* provides an appropriate foundation for the construct Professional Intelligence Judgement Artistry.

**THE STUDY**

The purpose of this research is to examine the processes of intelligence analysis using a construct of Professional Intelligence Judgement Artistry (PIJA). How is PIJA demonstrated? What frameworks do analysts use to make decisions? What forces internal and external might contribute to or influence the analytical process? For the purpose of this study intelligence analysis has been limited to the domain of law enforcement intelligence in order to create a coherent context for the examination of analytical decision-making. However law enforcement has not been limited to policing but includes those government agencies that have compliance and regulatory functions and maintain an intelligence capability.

This study is utilising a qualitative research paradigm to both define and refine the construct PIJA. This approach allows the research to be conducted in the real world, examining the construct of PIJA in its full context (Bowen, 2005; Ehigie & Ehigie, 2005; Krauss, 2005). In the case of the PIJA construct, it is argued that its complexity necessitates the extraction of meaning for the purpose of understanding rather than proving. Moreover this research fits the ‘naturalistic’ ontology as described by Bowen (2005) in that it is being conducted in the natural setting, utilising qualitative methods, purposive sampling and inductive analysis. This approach is considered appropriate in the case of this research as it is exploratory research into the phenomenon of intelligence analysis.

There are significant differences between domains examined in previous research, Occupational Therapists are tertiary trained and recognised as professionals whom it may be argued have a common foundation in terms of understanding professional outcomes within their field. Furthermore they are regulated by governing bodies, require certification and represented by professional bodies as is the case across the wider medical domain and with education. A similar case it may be argued exists in the management domain (Grainger, 2003; Paterson, 2003; Sadler-Smith & Smith, 2006). Intelligence analysts however do not have to undertake formal education to prepare them for employment, there is significant variation in the employment of intelligence analysts and whilst there is some common foundation in terms of professional capability or understanding, there are quite significant variations across the profession. Evetts (2006) posits a view as to how to recognise or define professions suggesting that they may be categorised by virtue of the fact that they operate in the knowledge environment, focus on the uncertainties in risk societies and are ostensibly dealing with risk and risk assessment to support a client’s management of uncertainty. Intelligence is and has historically been focused on determining risk exposure and reducing uncertainty. Rodgers (2006) and Marrin and Clemente (2005) in seeking to address the issue of intelligence as a profession argue that there are striking similarities between the profession of intelligence and that of medical and mental health practitioners in terms of the approach to diagnosis and analytical prediction. Therefore for the purpose of this study intelligence will be deemed a profession.

A pilot study comprising three interviews was conducted during September / October 2009. The three participants were selected for their breadth of experience across multiple law enforcement agencies. The analysts referred to hereafter as W1 through W3 are described below:

- W1 has been working as an analyst for six years primarily in the policing environment. W1 has an undergraduate degree in computer science and has completed a course work Masters of Information Security and Intelligence.
- W2 has been employed as an analyst for eight years now and has worked in policing, anti-corruption, the private sector and a compliance role in state government. W2 has completed an undergraduate degree in criminology. In addition to operational analytical roles W2 also has experience in the delivery of intelligence training within the law enforcement domain.
- W3 has been employed as an analyst for nineteen years and during this time has worked in state and federal agencies primarily within the law enforcement domain. W3 has completed a Graduate Diploma in Criminal Intelligence. In addition to the operational roles held by W3 he has been involved in the delivery of intelligence training within the law enforcement domain.

The interview process consisted of semi-structured interviews, each lasting approximately 50 minutes and addressed nine themes as shown in the table below. Each theme was explored in conversation with the subject and issues of interest teased out through a series of sub questions appropriate to the theme being explored at the time. All interviews were subsequently transcribed by the researcher. Initial analysis has consisted of identifying key concepts to emerge from the interviews.

Background, experience & history of the analyst	The concept of analysis	Decision & judgement in analysis
---	-------------------------	----------------------------------

Art, science, craft of analysis	Expertise and analysis	The analyst, average and outstanding
Professional artistry	Ethics & analysis	General thoughts

**DISCUSSION OF EARLY FINDINGS**

Due to the very early stage of this research the discussion of responses to the themes will be limited primarily to some interesting insights pertinent to the context of professional artistry. In the first instance though it is worth looking briefly at what might be described as the serendipitous entry into the world of intelligence as all three analysts were very quick to highlight their accidental entry into the profession. Moreover all three analysts when describing their career actually focus on the serendipitous nature of their entry into the profession. Notwithstanding this accidental career choice all discuss their profession with an obvious passion. The statement by W1 below clearly demonstrates this aspect of accidental entry into the profession.

*“Well I fell into it by accident, to be honest, [ ] I didn’t even know such a job existed when I was going through high school, Uni as a career path.”*

This accidental nature of entry into the profession has come as something of a surprise however its significance at this early stage is not certain. Its relevance may be more specific to the concept of intelligence as a profession rather than professional artistry, it is however an issue that will be explored further as the study progresses.

**Experts, expertise and analysis**

The concepts of the intelligence experts and analytical expertise were discussed with each participant. W1 suggested that the domain of intelligence was one in which experts cannot really exist whereas W3 was of the opinion that expertise was something quite narrow and contained within a specific context. Overall there was reluctance to use the label expert in regards specific intelligence analysts. Whereas on the issue of intelligence analysis both W2 and W3 focused on what they perceived to be an incongruity in that you analyse information in order to produce intelligence. However all three agreed that intelligence analysis was also about creating context out of voluminous data. Generally the participants’ description of analysis as a process was consistent with the literature. Lefebvre (2004) describes the process of intelligence analysis as being one of evaluation and transformation of data into a product for the use of policy consumers who may more broadly be defined as being decision makers. Critically it involves “assessing the reliability and credibility of the data, and comparing it with the knowledge base available to the analyst, to separate fact from error and uncover deception” (Lefebvre, 2004, p. 236). Gill and Phythian (2006) suggest that analysis is a process of seeking knowledge and assigning certainty sufficient to allow decision makers to act on the intelligence provided. More generally analysis is recognised as being an intellectual process focused on identifying truths, making appropriate judgements and explaining the evidentiary basis of such (Atran, 2006; George, 2004; Herbert, 2006; Heuer, 1999; Moore, 2007; Moore et al., 2005). It was therefore expected that the study participants would also describe their own profession within a similar context and this proved to be the case. However a somewhat unexpected finding was the degree of superficiality of understanding of those various concepts as they relate to the profession of intelligence. It is possible that this reflects the fact that there is no core professional knowledge base for the profession and is a key point of difference with professions such as medicine, occupational therapy and education.

**Self as an analyst**

According to Schon one of the keys to higher level competence or excellence is the ability to reflect on one’s own knowledge and experience (1992). It was therefore expected to some degree even in these exploratory interviews that participants would have in the course of their career reflected on what they know and what they do however responses seemed to suggest this had not really occurred. When queried, on their decision-making and judgement processes all three analysts struggled to find words to describe how they made decisions or formed judgements. Whilst all could describe a process when it came to framing their actual decision making and judgement they introduced terms such as experience and intuition. W1 and W2 described it as just something they have come to know and to some degree something they had not really given much thought to previously. Whereas W3 struggled to articulate it as clearly as he wanted yet at the same time did clearly demonstrate evidence of significant reflection on the issue. The Analysts were asked to describe or explain how concepts such as art, science and craft related to intelligence and in particular how it related to themselves as analysts. W1 struggled with this and tended to consider art and science in very concrete terms. This may be representative of his lack of experience or possibly a reflection of his employment in the tactical domain of intelligence. Having considered the issue of intelligence as an art, science or craft W2 when seeking to describe it was inclined to put it into the context of what made an outstanding analyst outstanding, W2 linked artistry to experience. Whereas W3 had some specific views as to how this related to the development of analysts and a strong view that you can’t make an analyst unless they have certain basic aptitudes. Generally concepts of art and science as it related to analysis were understood at a relatively superficial level. However in the case of W3 there were some fairly clear distinctions as to where art and science fit in the analysis framework. In W3s case science was something that dealt

with technology applications to intelligence whereas art represented the human aspect on analysis. W3 suggested a link between art and aptitude and suggested that it was the art aspect that was necessary for higher level analysis. This is in keeping with the observations of Paterson in relation to excellence in Occupational Therapy(2003).

### Separating average from outstanding

When asked to describe an outstanding analyst W2 and W3 both were able to quite clearly articulate many of the aspects that separated the outstanding analyst from the average whereas W1 struggled somewhat. W1 in fact seemed to have a more superficial understanding of what the differences may have been. That said W1 recognises that there is element of going beyond the requirement possibly anticipating intent of the intelligence client. With regard the concept of the average analyst all three were quite clear in their opinions that the average analyst is one whom has technical proficiency, capacity to complete the task within specified parameters, utilised a pro-forma or template approach to completion of the task at hand. This compared with the outstanding analyst, whom demonstrated insight, perception, curiosity and passion for the task. This is in keeping with Schon (1992, p. 51) who introduces what he refers to as 'indeterminate zones of practice – the situations of complexity, the elusive task of problem setting' and the role of artistry in dealing with this. This professional artistry reflects the tacit experiential knowledge practitioners acquire. Knowledge they just know yet struggle to articulate. Paterson, Wilcox and Higgs (2006) build on the work of Schon and introduce the concept of "judgement artistry" as a means of explaining how individual practitioners integrate the breadth of their experience and knowledge, within the context of their environment to deal with highly complex problems. Grainger (2001) also builds on Schon's work and expands the meaning of artistry to encompass how professionals translate knowledge and theories irrespective of the domain from which they are drawn. In all cases the argument is that there is more to professional competence or expertise than learned technical competency. Based on the outcomes of these early interviews it does appear that the constructs of professional artistry and judgement artistry may prove to be an appropriate framework in which to assess the process of intelligence analysis.

## CONCLUSION

At this very early stage in the study with limited analysis of the interview data substantive conclusions as to what separates the average from the outstanding intelligence analyst cannot be stated. However even at this early stage there is evidence emerging that the means of identifying and understanding what separates the two states is the lens of *professional artistry*. Some scholars and the study participants tend to be in agreement that good analysts possess certain qualities regardless of the domain they operate in (Gazit, 1980; Heuer, 1999). Those qualities include demonstrated intellectual capacity, curiosity, a degree of scepticism, and attention to detail. Additional qualities noted by the study participants include, creativity, tenacity, foresight and contextual understanding. These qualities are in keeping with those identified by Paterson (2003) in her study of occupational therapists and by Grainger (2003) in her study of professional artistry in teaching.

What has emerged from these interviews is a sense that intelligence analysis is at once complex and an intellectually demanding task. In order to operate effectively analysts need strategies to be able to cope with voluminous amounts of disparate data and ability to contextualise the problems they face. Unlike the investigators whom, in essence deal with facts the analysts deal with speculation, supposition, facts and a high level of uncertainty. Outstanding analysts in many cases identify the problem before the problem is recognised as such whereas average analysts are more process driven.

## REFERENCES

- Atran, S. (2006). A Failure of Imagination (Intelligence, WMDs, and "Virtual Jihad"). *Studies in Conflict & Terrorism*, 29(3), 285-300.
- Bowen, G. A. (2005). Preparing a Qualitative Research-Based Dissertation: Lessons Learned. *The Qualitative Report*, 10(2), 208-222.
- Cooper, J. R. (2005). *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*. Washington: Center for the Study of Intelligence.
- Cope, N. (2004). Intelligence Led Policing or Policing Led Intelligence. *British Journal of Criminology*, 44(2), 188-203.
- Ehigie, B. O., & Ehigie, R. I. (2005). Applying Qualitative Methods in Organizations: A Note for Industrial/Organizational Psychologists. *The Qualitative Report*, 10(3), 621-638.
- Evetts, J. (2006). Short Note: The Sociology of Professional Groups New Directions. *Current Sociology*, 54(1), 133-143.
- Gazit, S. (1980). Estimates and Fortune-Telling in Intelligence Work. *International Security*, 4(4), 36-56.
- George, R. Z. (2004). Fixing the Problem of Analytical Mind-Sets: Alternative Analysis. *International Journal of Intelligence and CounterIntelligence*, 17, 385-404.
- Gill, P., & Phythian, M. (2006). *Intelligence in an Insecure World*. Cambridge: Polity Press.
- Grainger, S. (2001). Accessing Professional Artistry: The Importance of Cooperative Education and the Limitations of Classical Research. *Asia-Pacific Journal of Cooperative Education*, 2(1), 1-5.

- Grainger, S. (2003). *Accessing the Professional Artistry of Teaching*. Griffith University, Brisbane.
- Grieve, J. (2004). Developments in UK Criminal Intelligence. In J. Ratcliffe (Ed.), *Strategic Thinking in Criminal Intelligence* (pp. 25-36). Sydney: The Federation Press.
- Herbert, M. (2006). The Intelligence Analyst as Epistemologist. *International Journal of Intelligence and CounterIntelligence*, 19(4), 666-684.
- Heuer, R. J., Jr. (1999). *Psychology of Intelligence Analysis*. Washington: Center for the Study of Intelligence.
- Johnston, R. (2005). *Analytic Culture in the US Intelligence Community: An Ethnographic Study*. Washington: Center for the Study of Intelligence.
- Krauss, S. E. (2005). Research Paradigms and Meaning Making: A Primer. *The Qualitative Report*, 10(4), 758-770.
- Lefebvre, S. (2004). A Look at Intelligence Analysis. *International Journal of Intelligence and CounterIntelligence*, 17(2), 231-264.
- Marrin, S. (2009). Training and Educating U.S. Intelligence Analysts. *International Journal of Intelligence and CounterIntelligence*, 22(1), 131 - 146.
- Marrin, S., & Clemente, J. D. (2005). Improving Intelligence Analysis by Looking to the Medical Profession. *International Journal of Intelligence and CounterIntelligence*, 18(4), 707-729.
- Moore, D. T. (2007). *Critical Thinking and Intelligence Analysis* (Vol. 14). Washington: NDIC Press.
- Moore, D. T., Kirzan, L., & Moore, E. J. (2005). Evaluating Intelligence: A Competency-Based Model. *International Journal of Intelligence and CounterIntelligence*, 18, 204-220.
- Paterson, M. (2003). *Professional Practice Judgement Artistry in Occupational Therapy*. University of Sydney, Sydney.
- Paterson, M., Wilcox, S., & Higgs, J. (2006). Exploring dimensions of artistry in reflective practice. *Reflective Practice*, 7(4), 455-468.
- Ratcliffe, J. H. (Ed.). (2004). *Strategic Thinking in Criminal Intelligence*. Sydney: The Federation Press.
- Rieber, S. (2004). Intelligence Analysis and Judgmental Calibration. *International Journal of Intelligence and CounterIntelligence*, 17(1), 97-112.
- Rodgers, R. S. (2006). Improving Analysis: Dealing with Information Processing Errors. *International Journal of Intelligence and CounterIntelligence*, 19(4), 622-641.
- Russell, K. (2004). The Subjectivity of Intelligence Analysis and Implications for the U.S. National Security Strategy. *SAIS Review*, XXIV(1), 147-163.
- Sadler-Smith, E., & Smith, P. J. (2006). Technical rationality and professional artistry in HRD practice. *Human Resource Development International*, 9(2), 271-281.
- Schon, D. A. (1992). The crisis of professional knowledge and the pursuit of an epistemology of practice. *Journal of Interprofessional Care*, 6(1), 49 - 63.
- Swenson, R. G. (Ed.). (2003). *Bringing Intelligence About Practitioners Reflect on Best Practices*. Washington: Joint Military Intelligence College.

## **COPYRIGHT**

Jeff Corkill ©2009. The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors

## **Terror attacks: Understanding social risk views between Singaporean lay and security practitioners**

Yam Hong Loo<sup>1</sup> & David J. Brooks<sup>2</sup>

<sup>1</sup>Singapore Manufacturers Association

<sup>2</sup>Security Research Centre (SECAU)

Edith Cowan University

### **Abstract**

*This study investigated the psychometric risk perception between lay people and security practitioners towards terrorist attack against Singaporean educational institutions. Being located in Southeast Asia, Singapore is not immune to terrorist attacks from rebels found in the region. To promote fear and chaos, terrorists have begun to attack private and neutral institutions in order to promote their cause. Mosques, hospitals and other such institutions are no longer immune from terrorist attacks. The psychometric risk paradigm offers a basis for examining empirical views towards potential terrorist attack against such institutions. Survey data in comparing terrorist attack against Singapore's educational institutions with five other criminal activities were collected from two cohorts of 100 college students (considered as lay people) and 100 security practitioners. The study demonstrated that the students had a higher risk perception when compared to the security practitioners that terrorist attack against educational institutions in Singapore could occur, resulting in increased levels of dread and reduced feelings of control. Findings from the study supported previous studies that, in particular, there are differences between lay and practitioners views of risk, with practitioners' generally rating risk lower than lay people.*

### **Keywords**

Security, risk perception, psychometric, terrorist, educational institutions

### **INTRODUCTION**

The terrorist attacks on the World Trade Centre Twin Towers in New York on the 11<sup>th</sup> September, 2001, indicates that today terrorists' strategies, motivations, objectives, modus operandi and targeting have radically changed. In particular, the pervasive use of suicide bombings against innocent civilians, in advancing their multifaceted cause. Soft sites appear to be targets of attacks, as seen in recent years educational institutions are not spared from these attacks. From day-care centres to universities, all have the potential to be targeted by terrorist (Dorn & Dorn, 2006, p. 31).

In order for policy makers to apply appropriate security mitigation strategies, understanding risk perception is important. Everyone in their daily lives is exposed to risk and how people perceive risk, results to some degree in their decisions-making. People are generally less acceptable of risk if it is imposed by external factors over which they have no control. Several studies (Siegrist, Cvetkovich & Roth, 2000; Siegrist, 2000) have shown that understanding of people's perceptions of risk is important in order to make sound policy decisions.

The study analysed the understanding of the public's risk perception on terrorist attack against educational institutions located in Singapore, with the use of the psychometric risk as the theoretical framework. The study observed whether risk perception differed between the two selected cohorts, defined as lay people and security practitioners. Such information may assist government, security industry and academia to better understand the risk perception of their citizens, resulting in more suitable communication to the public.

In the study, the following Research Questions were considered:

1. What are the risk perceptions of Singaporeans regarding terrorist attack against educational institution?
2. Are there any significant differences in risk perceptions between the students and security personnel?

### **PERCEPTION OF TERRORISM**

There have been a number of international surveys involving perceptions of terrorism risk. Burns (2007) presented eight US studies relevant to the threat of terrorism. One of these asked respondents how likely and serious certain types of terrorist attacks may appear, for example airline hijacking, attack on public transportation, deliberate contamination of the food supply and release of a chemical or biological agent. The findings revealed that the respondents have substantial concerns about future terrorist attacks and that they would be willing to support policies that commit considerable resources to prevent future attack.

Holmberg and Weibull (2002) surveyed the Swedish population, finding that terrorism was the third most worrying threat. Another Swedish study by Bennulf (cited in Sjöberg, 2004) asked about *worry* and found terrorism ranked third. In that study, all the threats and hazards were concerned with violence and various life-threatening hazards, with no economic risks or other social risks mentioned. Nevertheless, Sjöberg (2004) found that in a study by Stutz (2002) demonstrated that the high level of perceived threat from terrorism among the Swedish public a year earlier had faded.

On 7<sup>th</sup> May 2009, the Singapore *Today* newspaper (Yeo, 2009) published a poll of 100 Singaporeans on “how concerned are you that a terrorist attack ... will happen in Singapore.” The Poll revealed that 52% expressed extreme concern or concern, while 33% expressed unconcerned or were extremely unconcerned that a terrorist attack will happen in Singapore. Such results appeared to indicate that Singaporeans were aware that they could be exposed to a terrorist attack. In the same news article it was highlighted that although Singaporeans had not experienced any major incidents, they were aware of the security threats around them due to the awareness instilled in them by Government (Yeo, 2009). It is important to note that terrorism’s future orientation highlights the importance of understanding how people respond to threats, as well as to actual incidents. The psychological study of risk provides insight into how people may react to the threat of terrorism (Jenkin, 2006).

**PSYCHOMETRIC RISK**

Psychometric theory of risk is a quantitative methodology of the study of human behaviour (Brooks, 2003, p. 20). It was Slovic (1992) who developed a method, which was termed the *psychometric paradigm* to study the risk perception of risk to certain activities and technologies. The origin of the psychometric paradigm is the expressed preferences approach developed by Starr (1969), which was developed as a method of weighting technological risks against benefits.

Fischhoff, Slovic, Lichtenstein, Read and Combs (1978) proposed a psychometric model of risk perception that initiated the psychometric risk paradigm. The authors compiled nine dimensions and asked people to rate the risk of 30 activities on each of the two dimensions. The nine dimensions were (1) voluntariness, (2) immediacy, (3) know to exposed, (4) known to science, (5) controllability, (6) newness, (7) chronic, (8) common/dread, and (9) severity of consequences. This psychometric research approach “has been used to study a broad range of hazards, including technological risks, activities, and food hazards” (Siegrist, Keller, Kastenholz, Frey & Wiek, 2007, p. 60).

As explained by Brooks (2003, p. 40), the construct of risk perception may be measured by two risk factors, being the *sense of dread* and the *sense of familiarity*. The measure of each factor defined the perceived level of perceived risk towards certain activities or technologies (Figure 1).

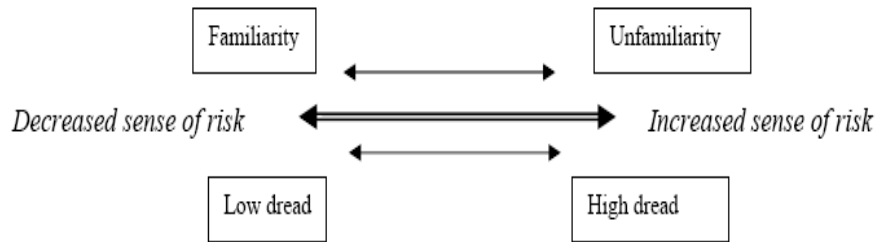


Figure 1 Psychometric risk perception factor model (Brooks, 2003, p. 40)

Through factor analysis, the two factors *familiarity of risk* and *dread risk* presented the underlying pattern of inter-correlations among the judged variables (Figure 2). Such studies (Slovic & Webb, 2002) exhibited the two factor analytical representation of 81 different activities and technologies, with factor one axis being defined as low dread risk to high dread risk while factor two axes being defined as unfamiliar risk to familiar risk.

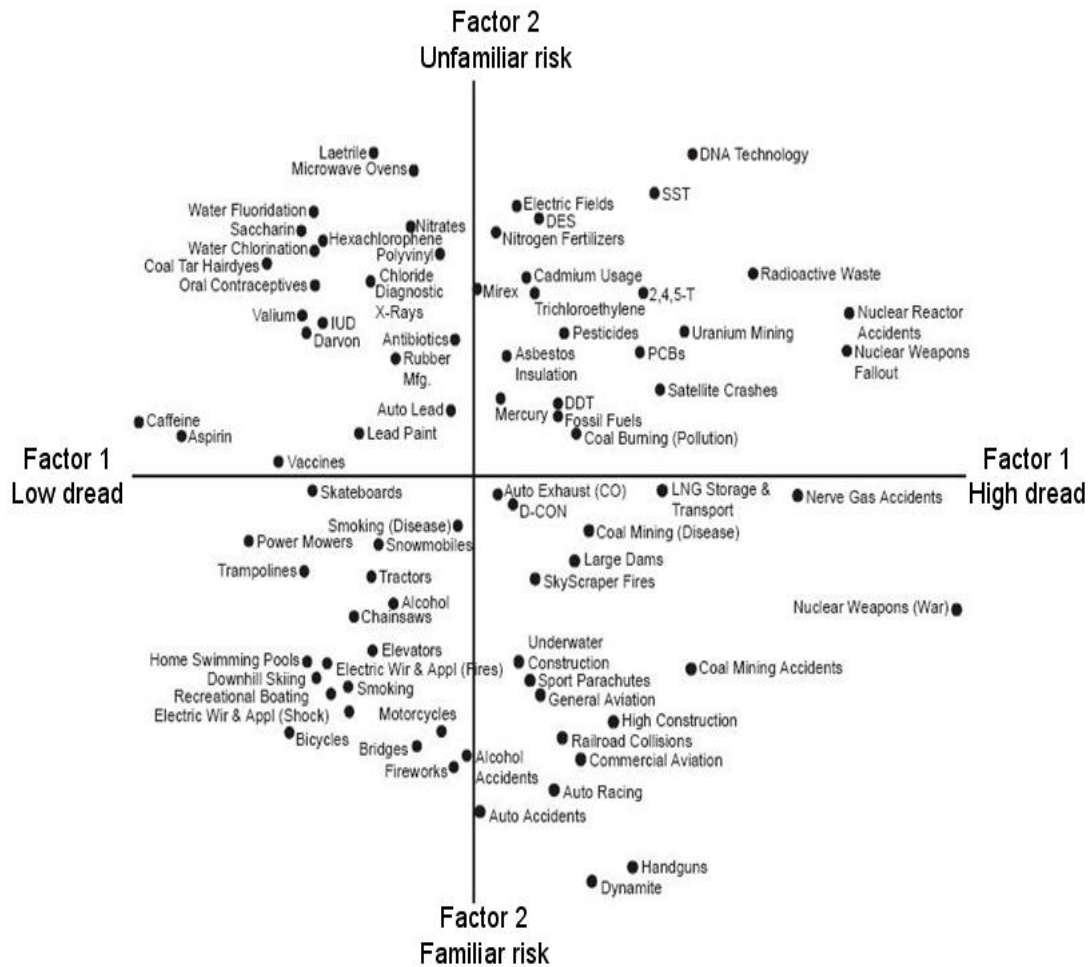


Figure 2 Psychometric paradigm: spatial locality of 81 hazards (Revised from Slovic & Weber, 2002, p. 11)

The two risk factors can be further expanded into the 18 characteristics of risk; however, for the purpose of this study, only nine of the 18 risk characteristics were tested (Table 1).

<i>Factor 2 – Dread risk</i>		<i>Factor 2 – Familiar risk</i>	
Low dread	Dread	Familiar	Unfamiliar
Controllable	Uncontrollable	Know to those exposed	Unknown to those exposed
Increasing	Decreasing	Old risk	New risk
Individual	Catastrophic	Effect immediate	Effect delay
Voluntary	Involuntary		

Table 1 The study’s nine measured characteristics (Revised from Slovic, Fischhoff & Lichtenstein, 2000, p. 142)

Although psychometric risk has been successfully applied to single hazards, Slovic (1987) cautioned against representing complex events as a single homogenous data point. While terrorism has been considered as a single hazard in previous psychometric studies, the complexity and relevance of terrorism in today’s society merits an empirical exploration of terrorism (Jenkin, 2006).

**Layman and expert differences**

Psychometric studies have shown that “perceived risk is quantifiable and predictable” and the “psychometric techniques seem well suited for identifying similarities and differences among groups with regard to perception and attitudes” (Slovic, 2000, p. 223). Therefore, the concept of risk is subjective and means different things to different people. One of the most significant findings within the psychometric paradigm is how lay people and experts distinguish between perceived and actual risk. “There is a mismatch in perception between the layperson and the industry expert” (Brooks,

2003, p. 21). *Experts* — and, consequently the policymakers who ask for expert advice — based their risk ratings on the expected number of fatalities. *Lay people*, in contrast, have a richer definition of risk (Marris, Langford, Saunderson & O’Riordan, 1997, p. 303) and consider a heuristic approach.

“The way people perceive risk, or risk perception, can be characterized as a battleground of strong and conflicting views” (Slovic, 1992, p. 54). As a result, conflicts may occur over the different definitions of risk concepts held by lay people and experts. Slovic (cited in Jenkin, 2006) explained such a discrepancy by concluding that experts view risk as the likelihood of actual harm based on mortality estimates, whereas lay perceptions of risk are based on a number of qualitative (and subjective) characteristics (p. 2).

**STUDY DESIGN**

A convenience sampling of students (n=100) and security practitioners (n=100) participated in the survey, which comprised of two parts. In the first part, the participants were asked to provide some demographic information, such as age, gender and occupation. In the second part, the nine risk perception characteristics (Table 1) were developed into questions and the participants asked to indicate their risk perceptions, based on the seven-point semantic differential scale (Figure 3). Five criminal activities, namely murder, kidnapping, armed robbery, rioting and burglary, together with *terrorist attack* against an educational institution were listed. Participants were asked to indicate their level of risk perception by marking the scale position.

<b>Criminal Activity 1 - Murder</b>												
Low Dread	1	2	3	4	5	6	7	High Dread				
<b>Criminal Activity 2 - Kidnapping</b>												
Low Dread	1	2	3	4	5	6	7	High Dread				
<b>Criminal Activity 3 - Armed Robbery</b>												
Low Dread	1	2	3	4	5	6	7	High Dread				
<b>Criminal Activity 4 - Rioting</b>												
Low Dread	1	2	3	4	5	6	7	High Dread				
<b>Criminal Activity 5 - Burglary (house breaking)</b>												
Low Dread	1	2	3	4	5	6	7	High Dread				
<b>Criminal Activity 6 - Terrorist attack against educational institution</b>												
Low Dread	1	2	3	4	5	6	7	High Dread				

Figure 3 Survey questionnaire using the risk characteristics

**Target population**

For this study, the study considered lay people and security practitioners who lived in Singapore and were ≥16 years old at the time of the survey. The sample population of lay people (n=100) were junior college students. Junior college students are post secondary students mainly in the age group of 18 to 19 years old preparing for the GCE ‘A’ levels examinations after two years of pre-university studies. The sample for security practitioners (n=100) consisted of full time qualified security personnel from local security agencies. Security personnel were chosen, as they have some cognisance and training in the area of terrorism and criminal activities. A particular security agency was selected for data collection, as all security personnel in Singapore have to undergo the Singapore Workforce Skills Qualification in security and thus there is some confidence that the sample accurately represented the security population.

**DATA ANALYSIS**

Data were analysed using the Statistical Package for the Social Sciences (SPSS) package. Descriptive statistics were generated to provide a risk profile for each of the sample cohorts, with independent t-test conducted to determine significance of the various risk perceptions.

**Risk characteristics**

The mean (M) and standard deviation (SD) for each of the risk characteristics were calculated (Table 2) by averaging all respondents (N=200) for the six criminal activities.

Characteristic	Murder		Kidnapping		Armed Robbery		Rioting		Burglary		Terrorist Attack	
	Mean	SD	Mean	SD	Mean	SD	Mean	SD	Mean	SD	Mean	SD
Dread	5.19	1.69	4.92	1.77	4.65	1.51	4.19	1.65	4.32	1.59	5.33	1.82
Control	4.63	1.86	4.16	1.77	3.93	1.73	3.71	1.78	3.17	1.75	4.77	1.78
Decrease of risk	4.30	1.49	3.62	1.48	4.20	1.42	3.62	1.64	4.24	1.42	4.20	1.81
Catastrophic	2.84	1.87	2.81	1.77	3.20	1.77	5.06	1.63	2.87	1.48	6.09	1.43

Voluntary	3.92	2.08	3.67	2.03	3.50	1.94	3.34	1.84	3.20	1.79	3.16	2.01
Risk knowledge	3.04	1.80	3.21	1.61	3.00	1.57	3.21	1.77	2.95	1.57	3.45	1.81
Severity conseq	5.51	1.65	4.71	1.58	4.34	1.56	4.31	1.63	3.56	1.65	5.70	1.56
Oldness/newness	2.54	1.88	2.80	1.83	2.58	1.59	3.04	1.83	2.49	1.46	5.28	1.80
Impact	2.63	1.63	3.28	1.82	2.70	1.51	3.27	1.77	3.24	1.67	2.56	2.00
Perceived risk	5.43	1.63	5.23	1.58	5.11	1.47	4.59	1.75	4.48	1.66	5.21	1.68

Table 2 Mean and standard deviation of the risk characteristics for each activity

These results (Table 2) revealed that the respondents perceived that a terrorist attack against an educational institution would make them experience the greatest amount of dread (M=5.33) when compared to the other activities. Rioting, however, would lead to the least amount of dread (M=4.19). As for the control over risk, the respondents indicated that during a terrorist attack, they would not be able to avoid death or injuries (M=4.77). Burglary (M = 3.17), on the other hand, were comparatively more controllable.

The respondents felt that the risk of all six criminal activities were in the neutral range (3.62 <M<4.30); however, a terrorist attack (M=6.09) was found to be catastrophic. Terrorist attack (M=5.70) and murder (M=5.51) were considered as having very severe consequence, while burglary (M=3.56) was seen as having the least consequence. Murder, kidnapping, armed robbery, rioting and burglary were considered old types of risk (2.49<M<3.04), while terrorist attack against an educational institution was considered a newer type of risk (M=5.28).

**Two-dimensional spatial factor representation**

A two-factor space *dread* and *familiarity* graph for the two participating cohorts (Figure 4) was plotted by averaging the means of the risk characteristics. Factor 1 dread are risks which are increasingly judged to be less controllable, increasing, more catastrophic and more involuntarily as you move from left to right of the graph. Factor 2 familiarity risks judged to be known, an old risk and having immediate effect.

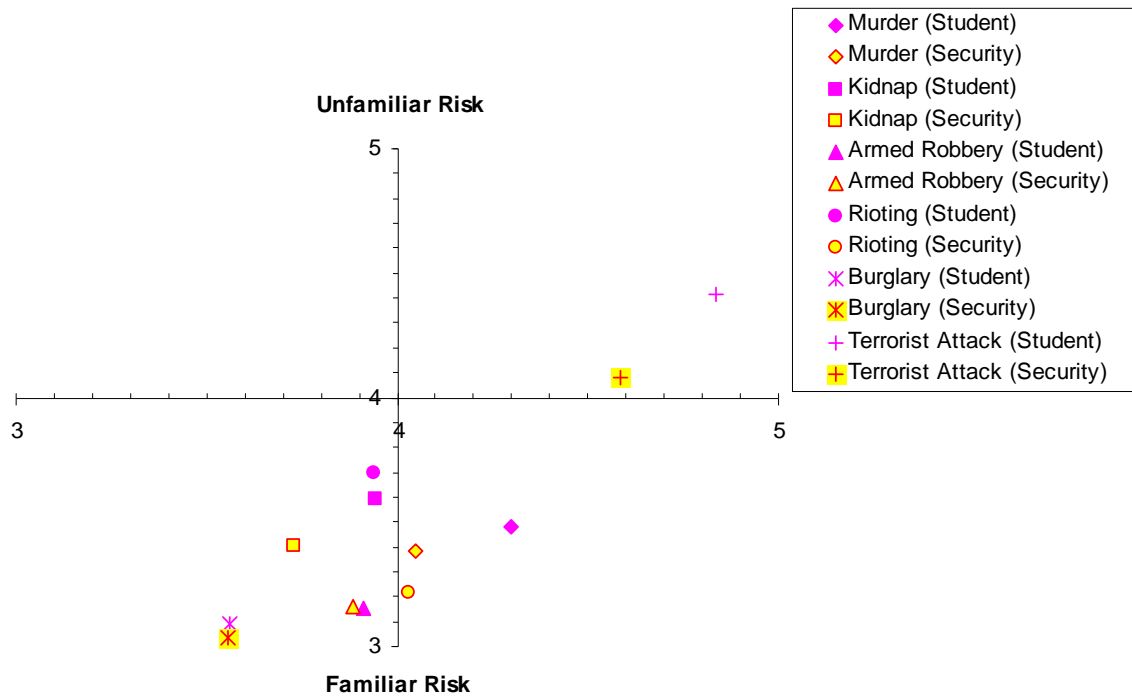


Figure 4 Risk perception map for student and security personnel

Both cohorts indicated similar spatial results, with the students showing slightly higher unfamiliarity of risk and higher dread risk for each of the activities than the security personnel. Nevertheless for terrorism, students indicated a significant higher dread and greater unfamiliarity to risk when compared to the security practitioners. For example, students had a significantly higher mean control over risk score (M=4.45) than the security personnel (M=3.67;  $t(198)=4.226, p=.000$ ) and a significantly higher mean severity of consequences score (M= 4.93) than the security

personnel ( $M=4.45$ ;  $t(198)=2.844$ ,  $p=.005$ ). On the other hand, the students had a significantly lower mean of risk score ( $M=3.81$ ) than the security personnel ( $M=4.25$ ;  $t(198)=-2.773$ ,  $p=.006$ ).

The findings (Table 3) indicated that the students had significantly higher mean scores than the security personnel in all activities. The student score for Murder ( $M=4.12$ ) was higher than the security personnel ( $M=3.88$ ;  $t(198)=2.374$ ,  $p=.019$ ). Students also had a significantly higher mean kidnapping score ( $M=3.96$ ) than the group of security personnel ( $M=3.73$ ;  $t(198)=2.044$ ,  $p=.042$ ). As for the terrorist attack, the students had a significantly higher mean terrorist attack score ( $M=4.70$ ) than the security personnel ( $M=4.45$ ;  $t(198)=2.725$ ,  $p=.007$ ).

Activity	Student (N = 100)		Security practitioner (N = 100)	
	Mean	SD	Mean	SD
Murder	4.12	.57	3.88	.83
Kidnapping	3.96	.70	3.73	.88
Armed robbery	3.77	.59	3.67	.77
Rioting	3.90	.75	3.76	.66
Burglary (house breaking)	3.46	.69	3.45	.67
Terrorist attack	4.70	.57	4.45	.73

Table 3 Activity ratings across cohorts

The alpha coefficient for the 10 risk characteristics (Table 4) were moderate (0.695 to 0.886). According to Cohen, et al. (2007, p. 506), these values indicated that the questionnaire was reliable and within the context of the study, for measuring the risk characteristics and the overall perceived risk.

Risk Characteristic	Alpha
Dread	0.886
Control over risk	0.855
Decrease vs. increase of risk	0.818
Individual vs. catastrophic	0.695
Voluntary vs. involuntary	0.897
Knowledge about risk	0.897
Severity of consequences	0.834
Old vs. new risk	0.812
Impact of risk	0.818
Perceived risk	0.822

Table 4 Internal coefficient Alpha for risk characteristics (n=200)

## THE PSYCHOMETRIC RISK MEASURE OF TERRORISM

The investigation describes the risk perceptions of lay people (student) and security practitioners (security personnel working in the security fraternity) regarding terrorist attack against Singaporean educational institutions. This measure was achieved by comparing the perceived risk of a terrorist attack against five other criminal activities, namely murder, kidnapping, armed robbery, rioting and burglary (house breaking).

### *Risk perception of terrorist attack against educational institution*

The first Research Question was designed to determine the risk perceptions of Singaporeans regarding terrorist attack against educational institution. The findings of this study suggested that risk was perceived differently among the six selected criminal activities. Therefore the participants perceived each criminal activity differently, perhaps as expected that some criminal activities were perceived as riskier than others.

In the two-dimensional spatial factor representation (Figure 4), two factors labelled as factor 1 dread risk and factor 2 familiar risk were used to describe the perceptions of the whole sample regarding a terrorist attack against educational institution against the other five criminal activities. For terrorist attacks dread risk was measured as *high*, resulting in a perceived dread, lack of control, more catastrophic outcome and that exposure to such attacks mat perceived as involuntarily. In addition, the perceived risk of terror attacks in the factor unfamiliar risk was measured as *high*, judged to be an unfamiliar risk, unknown and a new risk, and that any effect may be delayed. Terrorist attack against an educational institution was the only activity that scored higher than the neutral rating. It can thus be interpreted that Singaporeans judged the risk of a terrorist attack against educational institution as a high dread risk and an unfamiliar risk.

### **Differences in the risk perception of terrorist attacks**

The second Research Question was designed to determine whether there were any significant differences in the risk perceptions between student (laypeople) and security personnel. Based on the findings (see Table 3), the study concluded that risk perceptions differed significantly across students and security personnel in the area of risk control, knowledge about the risk and the severity of risk consequences. However, risk perceptions did not differ significantly across the two occupations for the dread or voluntariness of risk and whether the risk was old or new risk.

The study was able to conclude that the student perceived that the risk of a terrorist attack against an educational institution was greater than that felt by the security personnel. This result concludes that the practitioners, in general, rate risk lower than lay people, a view supported by past studies (Krause, Malmfors & Slovic, 1992; Barke & Jenkins-Smith, 1993; Slovic, Malmfors, Krewski, Mertz, Neil & Bartlett, 1995; Lazo, Kinnell & Fisher, 2000; Gutteling & Kuttschreuter, 2002). As Breakwell (2007, p. 71) concludes, there are substantial differences between lay and expert views of risk, with experts generally rating risks lower.

The key result in this study indicated that although terrorist attacks against educational institution fall in the high dread and unfamiliar risk quadrant, the mean score remained fairly close to the neutral point. This suggests that Singaporeans perceived a fairly neutral sense of riskiness and concern that an attack by terrorist on educational institution could occur. Such mentality could be due to the perception that Singapore is a relatively safe and orderly country, with low crime rates when compared to the other neighbouring countries. Singapore has also been spared from the direct experiences of terrorism that neighbouring countries like Indonesia and Philippines have had. In addition, that the Singapore Government is perceived to be highly regarded as efficient and capable with various law enforcement agencies having high trust level from the members of the public in preventing such incidents.

### **CONCLUSION**

The study has demonstrated that the perception of a terrorist attack in Singapore is *high*, when compared against the other measured risks. It is therefore pertinent to derive an effective risk communication strategy, devoting resources in engaging the public in risk dialogue so that they are more aware of such risks. Government agencies dealing with security risk management must know that they cannot properly reduce risk without first understanding how risk may be perceived. For the terrorists, mass killings and damage to property are only one-part of a larger plan to intimidate and paralyse the populace. Although each terrorist attack instils fear and intimidation, terrorists achieve some of their goals of psychological impact through the threat of future attacks, rather than solely through attacks that have already occurred. Although there has not been any terrorist attack against Singaporean educational institutions, it is still important to understand how people perceived the threat of terrorism, so that policy-makers are better able to develop national multi-layered defences against such risk.

### **REFERENCES**

- Barke, R., & Jenkins-Smith, H. (1993). Politics and scientific expertise scientists, risk perception, and nuclear waste policy. *Risk Analysis*, 13, 425-39.
- Breakwell, G. M. (2007). Individual and group differences in risk perception. *The psychology of risk*. London: Cambridge University Press.
- Brooks, D. J. (2003). *Public street surveillance: A psychometric study on the perceived social risk*. Australian Digital Theses Program, Edith Cowan University, Perth, Western Australia.
- Burns, W. J. (2007). *Risk perception: A review*. CREATE, Homeland Security Center. Retrieved 10 September 2008, from <http://create.usc.edu/research/54570.pdf>
- Cohen, L., Manion, L., & Morrison, K. (2007). *Research methods in education* (6<sup>th</sup> ed.). London: Routledge.
- Dorn, M., & Dorn, C. (2006). *Innocent Targets: When Terrorism Comes to School*. Canada: Safe Havens International.
- Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*, 9, 127-152.
- Gutteling, J.M., & Kuttschreuter, M. (2002). The role of expertise in risk communication: lay people's and experts' perception of the millennium bug risk in the Netherlands. *Journal of Risk Research*, 5, 35-47.
- Jenkin, C. M. (2006). Risk perception and terrorism: Applying the psychometric paradigm. *Homeland Security Affairs*, 2(2), 1-14.
- Krause, N., Malmfors, T., & Slovic, P. (1992). Intuitive toxicology: expert and lay judgements of chemical risks. *Risk Analysis*, 12, 215-32.
- Lazo, J.K., Kinnell, J.C., & Fisher, A. (2000). Expert and layperson perceptions of ecosystem risk. *Risk Analysis*, 20, 179-93.
- Marris, C., Langford, I. H., Saunderson, T., & O'Riordan, T. (1997). Exploring the "Psychometric Paradigm": Comparisons between aggregate and individual analyses, *Risk Analysis*, 17(3), 303-312.

- Siegrist, M. (2000). The Influence of Trust and Perceptions of Risks and Benefits on the Acceptance of Gene Technology. *Risk Analysis*, 20(2), 195-203.
- Siegrist, M., Cvetkovich, G., & Roth, C. (2000). Salient Value Similarity, Social Trust, and Risk/Benefit Perception. *Risk Analysis*, 20(3), 353-362.
- Siegrist, M., Keller, C., Kastenholz, H., Frey, S., & Wiek, A. (2007). Laypeople's and experts' perception of Nanotechnology hazards. *Risk Analysis*, 27(1), 59-69.
- Sjöberg, L. (2004). *The perceived risk of terrorism*. Stockholm: Working paper series in Business administration number 2002:11
- Slovic, P. (1987) Perception of Risk. *Science*. Vol. 236, p. 281
- Slovic, P. (1992). Public perceptions of risk. *Risk Management*, 39(3), 54-58
- Slovic, P. (2000). Perception of risk. In P. Slovic, *The perception of risk* (pp. 220-231). London: Earthscan Publication Ltd.
- Slovic, P., Fischhoff, B., & Lichtenstein, S. (2000). Facts and fears: Understanding perceived risk. In P. Slovic, *The perception of risk* (pp. 137-153). London: Earthscan Publication Ltd.
- Slovic, P., Malmfors, T., Krewski, D., Mertz, C.K., Neil, N., & Bartlett, S. (1995). Intuitive toxicology II; expert and lay judgements of chemical risks in Canada. *Risk Analysis*, 15, 661-75.
- Slovic, P., & Weber, E. U. (2002). *Perception of risk posed by extreme events*. Canada: Simon Fraser University. Retrieved September 2, 2008, from [http://www2.sfu.ca/media-lab/archive/2004/226jan2004/notes/slovic\\_wp.pdf](http://www2.sfu.ca/media-lab/archive/2004/226jan2004/notes/slovic_wp.pdf)
- Starr, C. (1969). Social benefit versus technological risk. *Science*, 165, 122-123.
- Yeo, A. (2009). *S'poreans aware of threats*. The New Paper. Retrieved May 8, 2009 from <http://news.asiaone.com/News/The%2BNew%2BPaper/Story/A1Story20090506-139754.html>

## **COPYRIGHT**

Yam Hong Loo & David J. Brooks © 2009. The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

## Consensual security risk assessment: Overcoming bias, conflicting interests and parochialism

Benjamin Beard & David J. Brooks  
Security Research Centre (SECAU)  
Edith Cowan University

### Abstract

*In a risk assessment process, insular methods of data collection and analysis may lead to an inaccurate risk assessment as stakeholders hold individual biases, conflicting interests and parochial approaches to certain risks. The article considered these issues and tested a consensual risk assessment approach that can overcome many of these issues. A staged risk assessment process was applied within an entertainment complex in the Security, and Food and Beverage Departments. Eight supervisors from the two departments participated in the study, with each participants individually interviewed on their view of predefined risks followed by the same risks discussed within a facilitated group.*

*The study first identified a list of the twenty most important risks according to the two departmental managers. From this initial identification of risks, four supervisors from each department ranked, from highest to lowest, all twenty risks as individuals. Following this stage, the consensus activities involved four supervisors from one department who ranked all twenty risks as a group and with the aim that all participants had to agree. Finally, the consensus activity was repeated with all eight participants present. Such a staged approach allowed the various approaches and resulting outcomes from the various risk assessment methods to be compared. Such a comparison found that there was a need to gain common understanding or clear definition of risks within the group, that an individual's assessment of a risk was driven by their own perceptions and that less important risks held a more common view, whereas higher risk had a greater diversity of views.*

**Key words:** security, risk, assessment, bias, consensus

### INTRODUCTION

AS/NZS4360:2004 suggests that the risk assessment process should not be conducted or information gathered in isolation. Further to this view, HB167:2006 states that “people who work in an organisation often have very important information about weakness” (Standards Australia, 2006, p. 13). Taking an insular method of data collection may lead to inaccurate risk assessment, as stakeholders with vested interest may emphasise their own risks or worst, game the risk assessment process. Previous studies (Beard & Brooks, 2006) have demonstrated how a consensual risk assessment approach may result in a more acceptable risk assessment outcome when compared to individual assessments; therefore, this study further examined how this approach can be applied in another security risk management situation.

The field of risk management can be affected by small discrepancies in the information gathering process, resulting in significant impacts on the outcomes of a risk survey. To measure this affect, the research examined two methods of risk data collection in order to find the most appropriate approach. One method was *individual interviews* with the stakeholders. The second was a *facilitated risk meeting* with stakeholders to develop a consensus decision on risk. The method of data collection will be described and analysed, determining patterns and possible explanations.

### RISK MANAGEMENT

Risk management provides a sensible approach to managing risk (Fischer & Green, 2004, p. 130) and a generic guideline is AS/NZS4360:2004 Risk Management. AS/NZS4360:2004 is often considered “almost a de facto global standard” (Jay, 2005, p.2) and has become an international template on dealing with risk, having been used in Canada, United Kingdom, and translated into Cantonese, Mandarin, Japanese, Korean, French and Spanish (Jay, 2005, p. 3). Most recently, AS/NZS4360 became the template for the International Standards Organisation ISO/FDIS 31000. Many industries use this framework and its applications are as broad as financial, engineering and security risk management (Jones & Smith, 2005a, p. 2).

The standard's definition of Risk is the likelihood of an event taking place that will have an impact upon the objectives of the organisation (Standards Australia, 2004, p. 4), combining likelihood and consequence in determining the amount of risk through a structured and logical approach. AS/NZS4360: 2004 Risk Management is the industry standard document for conducting risk projects and because of this, it formed the framework for the methodology of this study. Its flexibility and broad scope allowed the framework to be applied to the research of consensual risk analysis, as it is “widely used by security professionals and risk managers across Australia” (Jones & Smith, 2005b, p. 2).

The Australian Standard stages of the risk management process instruct that all relevant stakeholders need to be included in the process. According to the Standard, stakeholders are “those people and organisations who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk” (Standards Australia, 2004, p.6). Further to this aspect is the need to take a “consultative team” approach (Standards Australia, 2004, p. 19); however, it can be argued that the standard does not present the necessity of providing a consensual assessment (Koller, 1999; Koller, 2000), with an appropriate methodology with a consensus based stakeholder meeting.

The consensus methodology is supported by Koller (2000, p. 67), when he asserted that “maximum benefit from the risk processes is realized only when multiple opportunities are consistently assessed or compared”, with a salient aspect of consistency being the arrival of a *consensus* (Koller, 2000, p. 68). The consensus approach may be supported, in particular for security risk, by the assumption that there is generally limited historical data. Without a consensus assessment, risks are assessed in isolation. Such an insular method of data collection and assessment may lead to inaccurate risk management, as stakeholders with vested interests may emphasise their *own* risks or *game* the risk assessment process. Also, assessors may bias the assessment process based on an individuals beliefs, perceptions and experience (Brooks, 2005).

## CONSENSUAL RISK MANAGEMENT

AS/NZS4360:2004 Risk Management states that all stakeholders need to be involved in the risk management process; however, it does not specify how although a consensual risk approach is one of the options available. A consensual approach to risk management would ensure that all risks are detailed and agreed upon by all stakeholders (Koller, 2000, p. 222). This approach involves a round table meeting with all stakeholders that needs to end in some degree of a consensual outcome. By using this model, issues such as individual risk perceptions can be minimised and their impact on the final risk assessment minimised. When conducting a consensus risk assessment, group dynamics will also have some role and an independent facilitator should conduct the activity, considered a group analysis or working group (Chapman, 1998). The methodology used by Beard and Brooks (2006, p. 8) into consensual security risk management has been modified to provide more valid outcomes and several stages added to build upon limitations of the original study.

Whilst AS/NZS4360: 2004 Risk Management is an overarching risk framework, one area where it could be improved is with greater detail in respect to involvement of stakeholders and how this should be achieved (Standards Australia, 2004, p. 11). This aspect is of concern because of people’s nature to adopt a parochial attitude towards their own vested interests. Heads of department will naturally try to skew risk assessments in their favour, ensuring budgets and structures remain or rise in their favour. This issue is of particular concern in the security industry, as *risk gaming* is a tool many security managers use in order to obtain approval from executive management for technologies they believe to be necessary and equivalent to the risk (Cubbage, 2005).

If skewed, biased or partially incorrect information is gathered in the earlier stages of the risk management process, than results at its completion will be invalid. The consensus approach should eliminate or reduce such discrepancies early in the risk assessment process by ensuring all parties agree and that no opinion overrides another. Such an approach should transcend many varying motives by gaining an outcome that is beneficial to all involved in the assessment (Koller, 2000, p. 228). Working group models have been successfully used to achieve an accurate and comprehensive risk management process and risk assessment in the construction industry (Chapman, 1998).

## LITERATURE REVIEW

The area of risk and risk management has been widely documented in many industries as a way of making projects and facilities safer and more efficient. The application to the security industry allows for placement of resources into areas most needed. Security risk assessment and management is described as a method to identify the risks and the probable effects that they will have on the entity being protected to minimise that risk to an acceptable level (Fennelly, 2004, p. 9). The field of risk management in security has slowly evolved over the last few decades (Standards Australia, 2006) and the methods used grown.

AS/NZS4360 Risk Management standard presents a framework (Figure 1) on how risk managers could conduct an assessment,, being recognised throughout the world and used in many different languages (Jay, 2005, pp. 2-3). The standard provides a solid framework for the risk management process, beginning with *Establish the Context*, where the scope is set, and all stakeholders identified and involved. Next, the risks are *Identified*, *Analysed* and *Evaluated* and finally, risks are *Treated*. Concurrently with the risk assessment stages, the process is *Monitored and Reviewed* with stakeholders constantly *Communicated and Consulted* (Standards Australia, 2004).

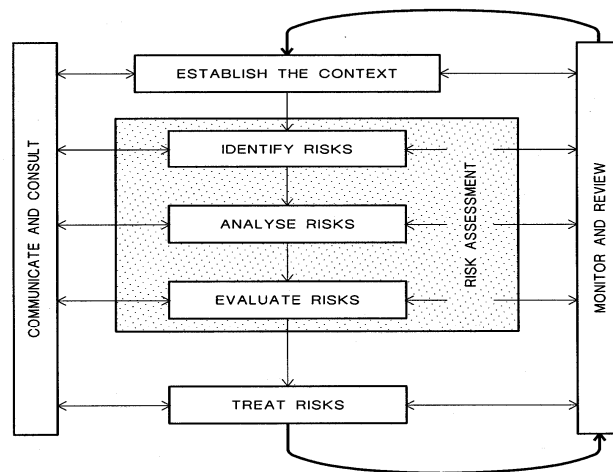


Figure 1 Risk management  
(Standards Australia, 2004)

The field of project management uses a large amount of risk assessment, and several methods of data collection that are poignant to both the security industry and this study. Kerzner (2003) stated that risks needs consideration in project management, along with costing and schedule. He favours several methods for achieving, this including:

- Individual interviews with stakeholders
- The Delphi method and
- The Nominal Group Technique (Kerzner, 2003, p. 666)

Individual interviews involve the facilitator gathering information from each stakeholder and then conducting the analysis and evaluation stages. The Delphi method firstly selects a panel of experts, consisting of decision-makers, staff and leading project staff (Turoff, 1970). Each expert makes an opinion on the chosen risk subjects, which is anonymously compiled by the facilitator. This feedback is redistributed to the panellists, who then make new opinions based upon the new information. The process is completed as often as is necessary to achieve the desired level of accuracy.

The Nominal Group Technique (NGT) was developed from social-psychological studies into decision-making in groups (Delbecq, 1968). The NGT is similar to the Delphi method; however, the participants have direct contact and all ideas are placed onto a flip chart without discussion. These ideas are discussed in the group and prioritised using a mathematical aggregate and repeated as often as necessary (Kerzner, 2003, p. 666). These approaches are used in the construction and project management industries; however, restricted research has been conducted into evaluating their effectiveness against the standard brainstorming technique proposed in risk management guidelines (Standards Australia, 2006) or their use in the specific security risk management field.

A study conducted an analysis of brainstorming techniques, namely the Delphi method and NGT using the model of the determinates of group effectiveness (Chapman, 1998; Handy, 1983). Chapman stated that there are three distinct categories of risk data collection; identification solely by the facilitator, the facilitator interviewing stakeholders and the facilitator leading a *working group*. Using the model proposed by Handy, Chapman compiled a list of the strengths and weaknesses of the three types of working groups (1998). In general, the study found that generating a group of participants that would work well together was very low regardless of the technique used. The use of these techniques in project risk management are documented; however, studies into *working group* techniques within security risk management are restricted.

One such study was considered by Beard and Brooks (2006) and their study into the use of a consensus approach in security risk management. Such a consensus approach involved gathering together all of the stakeholders in various departments of an organisation and working through the analysis and evaluation stages with the conclusion being a consensus, or all around agreement. By comparing this method with individual interviews and facilitator evaluation, it was found that a more rounded assessment could be gained with a consensus method. Otherwise participants tended to adopt a parochial attitude towards risk that affected or could be considered relevant to their own department (Beard & Brooks, 2006). This study used this approach to develop a methodology and analysis of a consensus approach. The overall goal was to create a set of identified and analysed risks, with relevant treatment options regarding security and liquor licence requirements.

## STUDY DESIGN

The design for the study (Figure 2) outlines the AS/NZS4360:2004 risk management framework (Figure 1) as the foundation for the study. Following this initial approach, the subsequent stage involved individual risk analysis for two distinct departments, with the final stage containing a consensus approach to risk analysis for Department 1 and both groups.

The study applied the risk assessment process in a large entertainment complex, within the Security Department (Department 1), and Food and Beverage Department (Department 2). The scope for the risk assessment process and the identification of the most significant risks concentrated on risks that affected both departments concerning infringements under the Liquor Licensing Act and the possible loss of the complex license. Eight supervisors, four from each department, participated in the study.

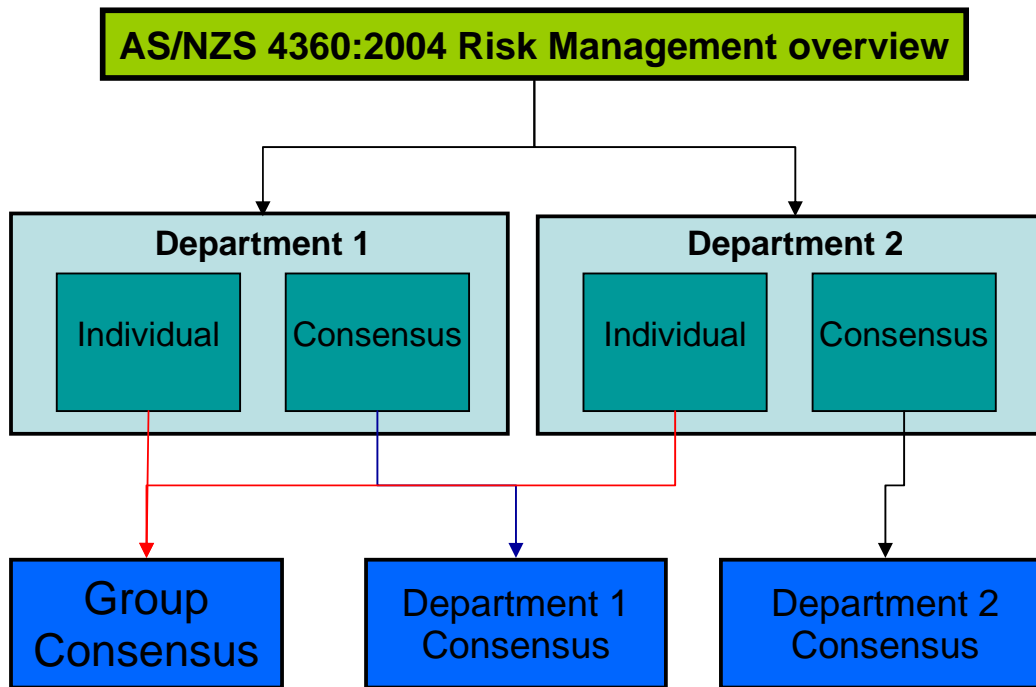


Figure 2 Study design

The study commenced with consultation with the site managers from both departments, with regard to the suitability and practicality of conducting the study. In addition, the scope for the identification and analysis of the risks was defined. In order to achieve a thorough research methodology, a pilot study was completed. This pilot study required a brainstorming session with the managers to create a list of ten risks. Using these 10 perceived risks, the managers individually listed the risks in order of highest to lowest (Cohen, Manion, & Morrison, 2000, p. 252). Again, using the 10 perceived risks, the managers ordered the risks by working together and arriving at a consensus of the risks from the highest to lowest. The results and comments gathered from this activity were used to improve the methodology for the larger group activities.

The first stage of the prime study was to identify the risks involved in the assessment, achieved with the assistance of the department managers (Standards Australia, 2004, p. 16). The managers brainstormed a list of twenty important risks that were to be assessed. These risks were listed on a survey form for the individual assessment activity and embedded into handout documents for the consensus activities. Following identification of risks, two methods of risk analysis were used and a comparison made. As individuals, four supervisors from Department 1 ranked all twenty risks from highest to lowest, repeated with four supervisors from Department 2.

The consensus activities involved arranging a meeting with all four supervisors from Department 1 that took part as an individual activity and having them rank all twenty risks. This activity was completed with a consensual outcome, as all participants had to agree as near as was practicable. Again, the activity was repeated with all eight participants present, which took longer due to the wider differences of opinion in the larger number of participants. The final stage for this activity was to discuss treatment options for the top five ranked risks.

## ANALYSIS

The analysis of the primary data (Table 1) presents the average results for both the department’s individual assessments, as well as the average of the individual assessments, Department 1’s consensus assessment and the combined consensus assessment.

<b>Risks</b>	Department1 Av	Department2 Av	Individual Av	Department1 consensus	Overall consensus
Risk A	9.5	16	14.75	8	17
Risk B	11	12.75	13.25	1	2
Risk C	4.75	5	5.5	4	1
Risk D	10.75	9	9.875	11	14
Risk E	5.5	7	6.25	12	11
Risk F	15	11	13	15	8
Risk G	9.25	4.5	6.875	6	9
Risk H	4.25	4.25	4.25	5	4
Risk I	17.25	17.75	17.5	17	20
Risk J	8	7.5	7.75	13	12
Risk K	13.25	9	11.125	16	13
Risk L	13.25	14.5	13.875	9	15
Risk M	5.25	4	4.625	2	5
Risk N	10.75	9.75	10.25	14	6
Risk O	5.25	11.5	8.375	3	3
Risk P	14.25	15	14.625	19	16
Risk Q	8.75	9	8.875	10	10
Risk R	19.25	15	17.125	20	19
Risk S	17.5	16.75	16.25	18	18
Risk T	7.25	10.75	9	7	7

Table 1 Risk comparison between departments

In considering the differences between the collected data (Table 1), the views of the two departments are similar to some degrees. There is however some large variances when comparing the individual assessments to the two consensus assessments. When comparing the average individual security response to the security consensus, the results are relatively similar with some exceptions such as *Risk E* and *Risk J*. The combined consensus group results, when compared to the other results, demonstrate the most difference. Whilst most of the risks remain ranked in the same quartile, there was noticeable movement in the rankings.

The average risk rankings from the Department 1 individual responses, the Department 2 individual responses and an all responses were calculated. These results show that the individual risk rankings between the two departments did not vary as much as anticipated. *Risk A* and *Risk O* were the only risks with a significant discrepancy between the two departments.

The standard deviation of each cohort were extracted (Table 2). The lower the value of the standard deviation in the combined individual results, the more aligned the individual assessments are. This demonstrates that risks such as *Risk I* and *Risk K* are ranked in the consensus, as all of the participants had similar individual rankings and the variance between the assessments was low (2.67; 3.31). Nevertheless, there were risks with higher standard deviation values, such as *Risk D* (6.62) and *Risk B* (6.99), with a lower degree of consensus in the group activities. The differences between the two department’s standard deviation values and the combined consensus values could indicate that there is differences in the departments with high values and that a particular risk, with a low standard deviation value, is considered equally by all members of the group.

<b>Risks</b>	Consensus	Department1	Department2	All individuals
Risk A	17	5.06	4.83	5.75
Risk B	2	6.68	8.22	6.99
Risk C	1	3.20	2.58	2.69
Risk D	14	7.41	6.73	6.62
Risk E	11	2.38	3.74	3.01
Risk F	8	4.08	5.94	5.18

Risk G	9	2.36	3.10	3.60
Risk H	4	2.87	2.62	2.54
Risk I	20	1.25	3.86	2.67
Risk J	12	5.35	5.68	5.11
Risk K	13	1.50	3.36	3.31
Risk L	15	7.32	1.00	4.88
Risk M	5	3.50	3.55	3.33
Risk N	6	5.37	3.20	4.13
Risk O	3	3.59	5.80	5.57
Risk P	16	3.86	1.82	2.82
Risk Q	10	3.30	2.58	2.74
Risk R	19	1.50	6.68	5.02
Risk S	18	1.29	3.86	2.69
Risk T	7	4.19	3.30	3.96

Table 2 Risk standard deviation comparison between departments

## EVALUATION AND FINDINGS

The results detailed above demonstrate that the aim of comparing and contrasting the individual and consensual approaches to security risk assessment were achieved. Such an outcome allows several important assumptions to be made, including the need to gain common understanding or clear definition of risk within the group, that individual's assessment is driven by their own perceptions and that less important perceived risk held a more common view whereas higher risk had a greater diversity of views.

First, in conducting an analysis of risk management and assessment methods, the pilot study and scope and identification stages indicated that the situation and risks must be clearly defined. In addition, that the risk scope carefully controlled in order to give appropriate results toward the risk assessment task. This study achieved this in two stages, which shaped the remainder of the methodology and activities.

Second, the individual approach to risk analysis appeared to produce varying results in the risk rankings. Whilst this was expected, due to individual opinions, there were very few patterns in the differences in each department. Such limited differences infer that the participants did not adopt a parochial attitude towards the risks that affected their area the most. This appeared to contradict previous results, which purported that people skew risks to favour their interests (Beard & Brooks, 2006). Overall, the averages of the individual risk rankings did not vary greatly from the individual department average or combined individual averages. Such an outcome supports the argument that the participants from all departments viewed the majority of the risks with the same attitude and therefore, consensus results from both the individual and the combined rankings.

Nevertheless, the consensus rankings are slightly different to the results found in the individual results, perhaps caused by the collaborative thinking and discussion of the risks. By using a group of people to discuss an issue, the result may broaden the participant's perceptions and curb any extreme views on the subjects. The two consensus activities' produced differing sets of results; however, the majority of risk movement was contained. Such a result may indicate that the two consensus groups were both regarding the risks with the same levels of concern, improving the accuracy of the combined consensus results.

The standard deviation adds an interesting outcome to the findings. These figures indicated that if a risk had a low standard deviation value in the individual rankings, it therefore had a strong and accurate rating in the consensus rankings. Such an outcome could be expected when considering a common measure and therefore, risk view. It is of importance to note that the risks with the lower standard deviation values also had a lower risk ranking, often in the last five ranked risks. This result could highlight that there was little discrepancy amongst the participants with regard to those risks that was considered the least importance. Therefore, the risk that had a high ranking and a higher standard deviation was considered important by the participant. In addition, the discussion in the consensus groups was especially exhaustive for the rankings of these risks. The standard deviation process could prove to be useful to management of organisations conducting risk assessment, as a method of gauging accuracy and effectiveness of risk rankings.

## LIMITATIONS OF THE STUDY

There were several elements of the study that could have been improved. The methodology was solid and well structured; however, there were minor problems with application due to the organisational aspects of having eight

managers of a busy company attend the one meeting. The reliability and validity aspects could have been addressed more thoroughly throughout the study. One approach to address the problem of validity would be to have a third group of participants conducting risk ranking and use this as a control group for comparison. To improve reliability, repeating the entire process at another organisation would provide another data set for comparison. Finally, a larger study that used the methodology presented in this study could be applied to a larger and more diverse group within or across several similar organisations. Such a study would further validate the findings and assumptions put forward in this study.

## CONCLUSION

Security risk management is increasing used to direct limited resources in the mitigation of threat; however, risk management can result in these limited resources directed in an inappropriate or less effective manner. Risk management should include a number of discrete steps, with risk assessment embedded within these steps and incorporating risk identification, analysis and risk evaluation. It is at this assessment stage that many factors may result in the risk management process being less than effective, including individuals perceptions of risk, parochial attitudes, invested interests, undefined risks, bias or a limited understanding of a risk. To overcome these issues, some form of group consensus should be achieved.

The article has presented a study that considered an approach that compared and contrasted individual and consensual approaches to security risk assessments. An organisation's group managers from two related divisions assessed a number of predefined risk, where the results were analysed and interpretations made. The study found that there was a need to gain common understanding or clear definition of risks within the group, that individual's assessment is driven by their own perceptions and that less important perceived risk held a more common view, whereas higher risk had a greater diversity of views. The study indicates that the use of different methods of risk assessment should consider the situation, using such approaches as group interviews, Delphi method and nominal group techniques. In addition, the results gathered from such group approaches can be used to ascertain accuracy and importantly, can confidently be used to allocate resources to minimise security threats.

## REFERENCES

- Beard, B., & Brooks, D. J. (2006). Security risk assessment: Group approach to a consensual outcome. *Proceeding of the 7th Australian Information Warfare and Security Conference*, 5-8.
- Brooks, D. (2005). Is CCTV a social benefit? A psychometric study of perceived social risk. *Security Journal*, 18, 19-29.
- Chapman, R. J. (1998). The effectiveness of working group risk identification and assessment techniques. *International Journal of Project Management*, 16(6), 333-343.
- Cohen, L., Manion, L., & Morrison, K. (2000). *Research methods in education*: London: Routledge.
- Cubbage, C. (2005). Module 1: introduction to security risk. [Handout]. Edith Cowan University, Perth.
- Delbecq, A. L. (1968). The world within the span of control, managerial behaviour in groups of varied size. *Business Horizons*, 11(4), 47-57.
- Fennelly, L. J. (2004). *Effective physical security*. Boston: Elsevier.
- Fischer, R., & Green, G. (2004). *Introduction to security*. (7<sup>th</sup> ed.). Boston: Butterworth-Heinemann.
- Handy, C. (1983). *Understanding organisations*. Middlesex: Penguin Books Ltd.
- Jay, C. (2005, 17 March). Big debacles help shape a new science. *The Australian Financial Review*, p. 2.
- Jones, D. E. L., & Smith, C. L. (2005b). *The development of a model for the testing and evaluation of security equipment within Australian Standard / New Zealand Standard AS/NZS4360:2004 - risk management*. Paper presented at the 2005 Recent Advances in Counter-Terrorism and Technology Summit, Canberra.
- Kerzner, H. (2003). *Project management: a systems approach to planning scheduling and controlling*. Hoboken: Wiley & Sons.
- Koller, G. (1999). *Risk assessment and decision making in business and industry: A practical guide*. Boca Ratan: CRC Press.
- Koller, G. (2000). *Risk modeling for determining value and decision making* Florida: CRC Press Ltd.
- Standards Australia. (2004). *AS/NZS 4360:2004 Risk management*. Sydney: Standards Australia.
- Standards Australia. (2006). *HB 167:2006 Security risk management*. Sydney: Standards Australia.
- Turoff, M. (1970). The design of a policy Delphi. *Technological Forecasting and Social Change*, 2(2), 149-171.

## COPYRIGHT

Benjamin Beard & David J Brooks ©2009. The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

## **Energy Security: An Australian Nuclear Power Industry**

Geoff I Swan  
secau -Security Research Centre  
Edith Cowan University

### **Abstract**

Climate change and energy security are driving a worldwide renaissance in nuclear power. An Australian nuclear power industry has also been seriously investigated by the Australian government and its agencies. This paper provides a broad overview of the nuclear fuel cycle and the nuclear power industry. It identifies aspects that are sensitive to nuclear terrorism and nuclear weapons proliferation to help security professionals identify threats and prepare for a possible Australian nuclear power industry.

### **Keywords**

nuclear power, energy security, uranium, radiation

### **INTRODUCTION**

It has been fairly widely accepted for decades in the scientific community that massive amounts of carbon dioxide (CO<sub>2</sub>) emitted into the atmosphere by humans would increase the “greenhouse effect” resulting in global warming and other climate change. The most recent fourth assessment report of the Intergovernmental Panel on Climate Change (IPCC, 2007) makes it clear that carbon dioxide is the most important anthropogenic greenhouse gas affecting the Earth’s energy balance, with the primary source being the burning of fossil fuels (coal, oil and gas). A global warming of 0.2°C per decade is projected over the next two decades and rises of several degrees this century are expected if CO<sub>2</sub> emissions are not reduced.

In Australia, over 96% of electricity generation (in terms of fuel inputs) is from coal, gas and oil (ABARE, 2009a). Hydroelectricity is our main “clean” electricity generation source which does not emit carbon dioxide. Although significant growth is likely in other “renewable” sources like wind generators, these are currently not suitable for base load power. Nuclear power plants can supply large amounts of base load power and do not emit greenhouse gases. With Australia’s natural wealth in uranium the nuclear option is being promoted, by some, as a “clean” source of base load power and an effective medium term action to reduce climate change.

The year 2006 was pivotal in Australia with a nuclear power industry being seriously investigated through two comprehensive reports. The first report was commissioned by the Australian Nuclear Science and Technology Organisation (ANSTO) to look at the economics of nuclear power in the Australian context (Gittus, 2006). In the second half of the year, a taskforce was appointed by the Prime Minister to investigate and report on uranium mining, value-added processing, and the contribution of a nuclear energy industry in Australia (Commonwealth of Australia, 2006). In summary, while high commercial and technology barriers could make Australian conversion, enrichment and fuel fabrication facilities difficult to build, there was support for an expansion of uranium mining, and nuclear power was considered economically feasible. The release in late 2006 of Al Gore’s academy award winning documentary film on climate change “An Inconvenient Truth” (2006), enhanced public perceptions of a crisis that is driving the debate on nuclear power in Australia.

Despite having huge natural energy resources, Australia could find its energy security under threat from the international community that may not accept our huge carbon footprint. Australia has recently overtaken the United States of America as the world’s biggest emitter of CO<sub>2</sub> per capita (Maplecroft, 2009), and globally enforced carbon emission caps may emerge as part of a global response to climate change. Australia may be forced to quickly reduce our reliance on fossil fuels or face sanction.

This paper provides a broad overview of the nuclear power industry with the nuclear fuel cycle described in sufficient detail for security professionals to better appreciate security issues. Reference will be made to those aspects of most concern for nuclear terrorism and nuclear weapons proliferation. Regulation, safeguards and international experience are also addressed.

## NUCLEAR FUEL

### Overview

Figure 1 shows a schematic diagram of the nuclear fuel cycle for nuclear fission power reactors. The front end of the nuclear reactor can be considered as two stages. Firstly, uranium ore is mined and processed to produce yellowcake ( $U_3O_8$ ). This normally occurs at or near the mine site. Secondly, specialist facilities are needed to enrich uranium and produce fuel that a nuclear power station can use to produce electricity. Finally, the spent fuel is managed through storage, reprocessing and waste disposal.

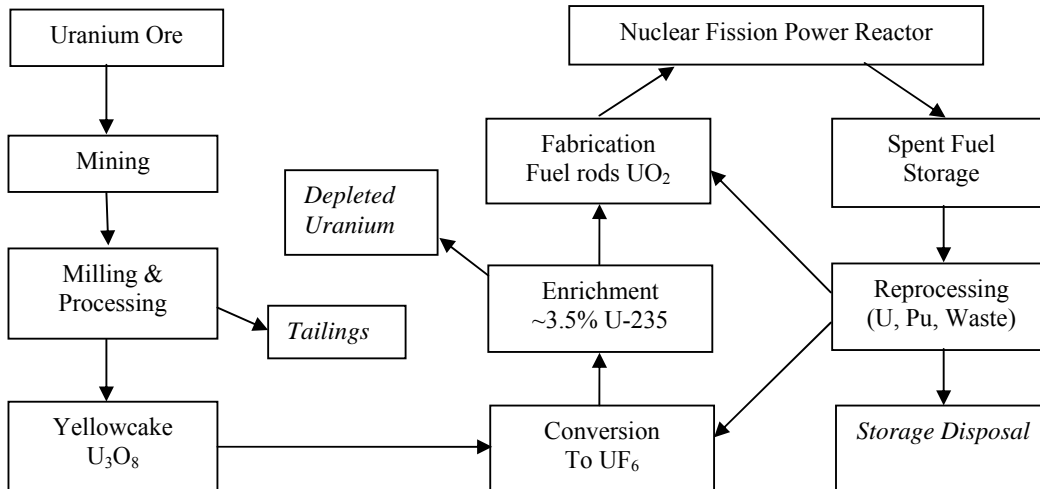


Figure 1. Schematic diagram of nuclear fission power reactor fuel cycle

### Uranium ore to yellowcake

Australia has the world's largest known recoverable uranium deposits (23%) in the world with major producers Canada and Kazakhstan account for about 60% of world supply of uranium for nuclear reactors from mines (World Nuclear Association, 2009). Natural uranium on Earth is radioactive and made up of 99.3% U-238 and just 0.7% U-235. Both U-238 and U-235 are alpha particle emitters with half lives of 4.5 billion years and 704 million years respectively (Thornton and Rex, 2006). The long half lives and dispersed nature of the uranium deposits make them not particularly radioactive. In the financial year 2007/2008, the three currently operating Australian mines at Ranger (NT), Olympic Dam (SA), and a small mine at Beverly (SA), produced a total of 10,101 tonnes of yellowcake (ABARE, 2009b). Yellowcake has a low specific radioactivity and is transported in 200 litre drums and loaded into shipping containers for enrichment overseas. World uranium mining will probably need to greatly expand in the coming decades due to an increasing number of nuclear power stations and a probable reduction in (currently 40%) nuclear fuel derived from decommissioned American and Russian nuclear warheads (ASNO, 2008) under the Treaty on the Reduction and Limitation of Strategic Offensive Arms (START).

### Conversion, enrichment and fuel fabrication

Through chemical reactions, yellowcake ( $U_3O_8$ ) is converted to uranium hexafluoride ( $UF_6$ ) before the technologically challenging task of enriching the U-235 abundance from its natural 0.7% to between 3% and 5%. This is necessary for use in almost all nuclear power reactors as it is the U-235 isotope that is fissile and can therefore produce energy. Whilst other enrichment methods have been used in the past or are under development, the centrifuge method now dominates the international uranium enrichment industry. When uranium hexafluoride is fed into a swiftly rotating cylinder (centrifuge) there is a slight separation of the isotopes with the lighter  $^{235}UF_6$  having a slightly higher concentration near the axis and the heavier  $^{238}UF_6$  having a slightly higher concentration in the outer regions. By withdrawing uranium hexafluoride from near the axis and repeating the process through a series of centrifuges the uranium hexafluoride can be enriched to reactor grade. The centrifuge method requires about one tenth of the energy required in the diffusion method that was common up to the 1970s. Urenco have been building a national enrichment facility in New Mexico to supply the US market using state of the art centrifuge technology with first production expected towards the end of 2009 (Urenco, 2009). After enrichment, uranium hexafluoride is converted to uranium dioxide ( $UO_2$ ) pellets for use as fuel in nuclear power reactors. Further details can be found in Bennet and Thomson (1989).

Enrichment of the U-235 isotope to between 3% and 20% is referred to as low-enriched uranium. Greater than 20% is high-enriched uranium with more than 90% considered weapons grade. Commercial enrichment technology and expertise could be fairly easily adapted to produce weapons grade uranium for use in a nuclear weapons program. Much effort is therefore devoted to restricting this highly sensitive dual use technology as a critical step in preventing the proliferation of nuclear weapons.

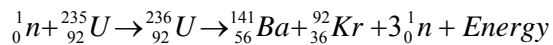
The usually unwanted U-235 deficient tails, known as depleted uranium, does have uses in other areas due to its chemical properties and high specific gravity of 18.7. It is found in counterweights (including keels of yachts) and in highly penetrating anti-tank ammunition.

## NUCLEAR POWER PLANTS AND SPENT FUEL MANAGEMENT

### Nuclear power plants

The World Nuclear Association (2009, August) reported that there are 436 operating nuclear power plants worldwide generating 372 GW of electricity. The two most common reactor types are the Pressurised Water Reactor (PWR) and the Boiling Water Reactor (BWR) with 260 and 92 plants respectively (Hore-Lacy, 2003). A succinct and up to date overview of current and proposed nuclear reactor types can be found in Norman, Worrall and Hesketh (2007).

At the heart of nuclear power is the induced fission process that occurs in the reactor core. When U-235 absorbs a thermal (slow) neutron, the compound U-236 nucleus created quickly splits into two daughter nuclei and two or three neutrons. One example of a neutron induced U-235 fission reaction is given below.



There are two important aspects to the nuclear fission reaction. Firstly the energy produced from U-235 fission is enormous and over a million times more than that produced by burning the same mass of coal. The daily requirements for a 1000MW power plant is about 3 kilograms of U-235 compared with about 8 million kilograms of coal (Thornton and Rex, 2006). Secondly, the fission produces neutrons that, when slowed down (moderated), may be absorbed by other U-235 nuclei to produce a self-sustaining nuclear chain reaction. Details of how the nuclear reaction is controlled, neutrons moderated, and heat energy transferred away to electrical generators can be found in most university level physics textbooks including those by Thornton and Rex (2006), Serway and Jewett (2008), and Halliday, Resnick and Walker (2008).

In addition to power reactors, there are over 250 research reactors in the world where the two primary functions are to produce high flux neutron beams for material science research and (through irradiation) manufacture radiopharmaceuticals for nuclear medicine. Some of these reactors use high-enriched uranium of up to 95% U-235, which unfortunately is also suitable for nuclear weapons. The new Australian research reactor, OPEL, uses low-enriched uranium (just) of 20%, which improves security and nuclear safeguards (ANSTO, 2005). Research reactors typically require higher enrichment than reactors optimised for commercial power generation. In addition, there are breeder reactors (Thornton and Rex, 2006) where fast neutrons from U-235 fission are absorbed by U-238, which then beta decays to produce (breed) Plutonium (Pu-239) that is also fissile. Inherent problems with breeder reactors make them relatively uncommon.

### Spent fuel management: storage and reprocessing

After 1-2 years, the used (or spent) nuclear fuel elements need to be removed from the reactor. Typically this used fuel is about 95% U-238, 1% Pu-239 (from transmutation of U-238 when a fast neutron is absorbed), 1% U-235, and 3% fission waste products (World Nuclear Association, n.d.). These waste products are highly radioactive and would be most dangerous if they were acquired by terrorists. Interim storage on site in large cooling ponds is required for several years to provide radiation protection, remove heat from further fission events, and (with the decay of short life radioactive isotopes) make the material easier to handle later.

The spent fuel is either moved for reprocessing (after a few years of interim storage) or is left as waste until final waste storage facilities are ready. Although technologies for storing waste more permanently are being developed, the current thinking is to place suitably sealed waste in deep and stable geological repositories. Former Australian Prime Minister Bob Hawke has recently called on Australia to consider developing a nuclear waste industry that could be a source of income and contribute to energy security worldwide given geologically safe and remote storage options (The Australian, 2009).

Reprocessing begins with the dissolving of spent fuel rods in acid to separate uranium and plutonium from the 3% waste products from the fission (World Nuclear Association, n.d.). These waste products are highly radioactive and require long term storage in drums. The uranium recovered can be recycled by going through the conversion and enrichment process again. It can also be used with the plutonium, which like uranium also produces energy through

neutron induced fission, to produce mixed oxide (MOX) fuel rods. One of many safeguards in a reprocessing plant is to avoid storing separated plutonium by mixing in a 50/50 ratio with uranium (Pickett, 2008)

## **SAFETY, NON-PROLIFERATION AND NUCLEAR TERRORISM**

### **Nuclear weapons: U-235 or Pu-239?**

Plutonium has clear advantages over uranium for the construction and delivery of nuclear weapons. Firstly, Pu-239 can undergo induced fission more easily than U-235 as it captures both slow and fast neutrons. Secondly, the Pu-239 fission reaction also produces on average 2.7 neutrons per fission compare with 2.3 neutrons for U-235. A runaway chain reaction is therefore easier to create for Pu-239 which allows for the development of smaller nuclear warheads that can be more easily delivered by ballistic missiles where size and shape are critical. Pu-239 is an alpha emitter with a half life of 24 thousand years and is highly toxic.

### **Pakistan and the Khan network**

The case of Pakistan and the Kahn network is illustrative of how easily technology and expertise can proliferate across international borders (Nuclear Engineering International Magazine, 2004). Back in the 1970's, Pakistan began acquiring enrichment technology including the design details for advanced Zippe-type centrifuges (after German Scientist Gernot Zippe) from a European enrichment facility operated by Urenco. Pakistan was able to develop its own enrichment capability and successfully tested a nuclear fission bomb in 1998. It is believed that this technology, through the Abdul Khan network, was sold on the black market to Libya, North Korea and Iran. Although Libya has since renounced its nuclear program, North Korea announced its first successful nuclear fission bomb test on October 9, 2006, and Iran, despite UN sanctions (UN Security Council, 2008), is expanding its uranium enrichment capabilities. Other Middle Eastern countries are also investigating the nuclear option.

### **Regulation and safeguards**

The International Atomic Energy Agency (IAEA) was established in 1957 as an independent organisation within the United Nations (UN) to promote safe, secure and peaceful nuclear technologies. The three main pillars of nuclear cooperation that underpin its mission are the promotion of safeguards and verification, safety and security, and science and technology. The IAEA has also responded to recent terrorist attacks through its coordination and strengthening of international approaches to promote nuclear security (IAEA, 2007).

Diversion of nuclear material and technology in the nuclear power industry to nuclear weapons programs is and has been a major problem and concern of the international community. The 1968 Non-Proliferation of Nuclear Weapons Treaty (NPT) aimed to restrict nuclear weapons to the five nuclear powers at the time: USA, Soviet Union (now Russia), China, France and the United Kingdom. Since the NPT came into force in 1970, India, Pakistan and North Korea have conducted nuclear weapons tests, Israel is believed to be a nuclear power and Iran is believed to be close to becoming a nuclear power. India, Pakistan and Israel have never been signatories to the NPT. South Africa was a small nuclear power before deciding to voluntarily disarm and Ukraine, Kazakhstan, and Belarus also briefly possessed nuclear weapons (Doyle, 2008). Given that much nuclear technology and expertise is common to the nuclear power industry and nuclear weapons programs, it has always been difficult for the IAEA, as the international body responsible, to inspect and verify solely peaceful intentions or operations. Additional protocols have been introduced to strengthen the non-proliferation safeguards in the NPT, but there was no general agreement to make these compulsory at the last five-yearly NPT review conference (NPT Review Conference, 2005). In September 2009 United States President Barack Obama chaired an historic summit of the security council which adopted resolution 1887 (2009) with 14 heads of state for broad progress on long-stalled efforts to staunch the proliferation of nuclear weapons and ensure reductions in existing weapons stockpiles, as well as control over fissile material (UN Security Council SC/9746, 2009).

In Australia, the Australian Safeguards and Non-Proliferation Office (ASNO) within the Federal Department of Foreign Affairs and Trade (DFAT) is charged with ensuring that nuclear materials and items are used only for authorised purposes and that our international treaty commitments, including the NPT, are met. ASNO also reports to the IAEA and arranges site visits. Australia's nuclear reactor at Lucas heights and three uranium mines with associated storage and transport operations are major responsibilities for ASNO. An Australian nuclear power industry would result in a huge increase in the storage and transport of radioactive materials. Further details of ASNO's role can be obtained in the 2007-2008 Annual Report (ASNO, 2008). Note that health and safety relating to radiation is mostly regulated by the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA, 2009).

### **Proliferation and nuclear terrorism**

Access to enrichment technology and expertise is the biggest stumbling block in producing the highly enriched U-235 required for a uranium bomb from uranium ore. Reprocessing technology of spent fuel rods from power reactors is

critical to extracting the Pu-239 required for the more versatile Plutonium bomb. It would seem logical that international and domestic concerns for the proliferation of nuclear weapons may limit the scope of an Australian nuclear power industry. However, a key finding of the second report (Commonwealth of Australia, 2006) is that increased Australian involvement in the fuel cycle would not change the proliferation risks or make Australia's energy grid more vulnerable to terrorist attack. Given international experience the author does not agree with this finding with respect to proliferation risks.

A nuclear power industry would create additional sources of highly radioactive material that would need to be secured at nuclear facilities and in transportation between facilities around the country. This material could be diverted for use in a Radiological Dispersal Device (RDD) to harm and terrorise a population. Natural disasters and accidental human intervention can also result in the dispersal of radioactive material (Swan, 2008). The ability to detect small amounts of radioactivity in a range of situations has become a bigger priority with increasing resources being allocated to tackle the problem. For example, in 2007 the Domestic Nuclear Detection Office (DNDO) of the US Department of Homeland Security (DHS) announced 10 contracts worth US\$8.8 million to perform exploratory research in advanced nuclear detection technology (DHS, 2007)

The difficulties of ensuring that access to sensitive information, materials, technology and critical people are appropriately controlled would be a substantial and complex undertaking for security professionals. For example, major infrastructure, like nuclear power plants and enrichment facilities would require high level physical security and effective policies and procedures for materials and personnel. Transportation of sensitive/dangerous materials over large distances is an issue and the monitoring and guarding of highly radioactive waste in remote depositories would also need to be addressed.

## AN AUSTRALIAN NUCLEAR POWER INDUSTRY?

The British Prime Minister recently signalled that he would like Britain to play a major role in building an extra 1,000 nuclear power stations around the world (The Independent, 2008). However, the change of federal government (from Coalition to Labour) in late 2007 has reduced the likelihood of Australia building nuclear power stations in the near future, although there is growing pressure within the ALP to more seriously revisit this option in response to climate change. In any case, the Australian uranium mining industry is preparing for rapid expansion and according to two recent comprehensive reports (Gittus, 2006 ; Commonwealth of Australia, 2006) nuclear power is a realistic option for Australia.

The ANSTO report (Gittus, 2006) concludes that nuclear power is demonstrably the safest way of generating electricity and is an excellent source of supplies. It is reported that the fatality rate per unit of electricity is one thousand times as great for coal, oil and gas than it is for nuclear. It is estimated that although the risk of a terrorist attack on an Australian nuclear power station is 50% higher since 9-11, the risk is still very low. This paper seeks to broadly identify critical segments in the nuclear fuel cycle for terrorism and/or proliferation that have the potential to cause great harm. The overall security risks are significant and would need to be mitigated.

Australia's current role in the world nuclear power industry is that of a major miner of uranium ore and exporter of yellowcake. Australia has no conversion or enrichment capability, no fuel fabrication facility, no nuclear power stations and no reprocessing facilities. Our reactor expertise revolves around the scientific use of one small research reactor at Lucas Heights near Sydney. An Australian nuclear power industry would require a huge influx of technology, expertise, and radioactive materials which together would have far reaching and complex security implications. Adapting from international best practice where possible, there would be a need to develop expertise for the Australian context to provide security for whatever segment of the nuclear industry we chose to develop. Finally, nuclear power is one of many highly politicised issues in Australia and that some elements of the community may choose to inflate or deflate public perception of risks to suit their own purposes.

## REFERENCES

ABARE (2009a, February). *Energy in Australia 2009*. Retrieved August, 2009 from [http://www.abare.gov.au/publications\\_html/energy/energy\\_09/energy\\_09.html](http://www.abare.gov.au/publications_html/energy/energy_09/energy_09.html)

ABARE (2009b, June). *Australian Mineral Statistics 2009: March quarter 2009*. Retrieved August, 2009 from [http://www.abareconomics.com/publications\\_html/ams/ams\\_09/ams\\_jun09.pdf](http://www.abareconomics.com/publications_html/ams/ams_09/ams_jun09.pdf)

*An Inconvenient Truth* [Film]. (2006). Paramount Classics, USA

ANSTO. (2005, June). *Open Pool Australian Light-Water Reactor (OPAL)*. Retrieved August, 2008 from [http://www.ansto.gov.au/\\_data/assets/pdf\\_file/0003/3558/OPAL\\_brochure.pdf](http://www.ansto.gov.au/_data/assets/pdf_file/0003/3558/OPAL_brochure.pdf)

ASNO (2008). *ASNO Annual Report 2007-2008*. Retrieved August, 2009 from [http://www.asno.dfat.gov.au/annual\\_report\\_0708/ASNO\\_2007\\_08\\_ar.pdf](http://www.asno.dfat.gov.au/annual_report_0708/ASNO_2007_08_ar.pdf)

- ARPANSA (2009). ARPANSA. Retrieved August, 2009 from <http://www.arpansa.gov.au/>
- Bennet, D. J., & Thomson, J. R. (1989). *The Elements of Nuclear Power* (3rd ed.). New York: John Wiley & Sons.
- Commonwealth of Australia (2006). *Uranium Mining, Processing and Nuclear Energy – Opportunities for Australia?*. Retrieved April, 2007 from <http://www.dpmc.gov.au/umpner/reports.cfm>
- DHS (2007). *DHS Awards \$8.8 Million for Exploratory Research on Advance Nuclear Detection Technology*. Retrieved August, 2008 from [http://www.dhs.gov/xnews/releases/pr\\_1174940537634.shtm](http://www.dhs.gov/xnews/releases/pr_1174940537634.shtm)
- Doyle, J. E. (2008). Dismantling Nuclear Weapons Activities: Politics and Technology. In J. E. Doyle (Ed.), *Nuclear Safeguards, security, and non-proliferation*. (pp.283-287). Burlington USA: Butterworth-Heinemann.
- Gittus, J. H. (2006). *Introducing Nuclear Power to Australia: An Economic Comparison*. Retrieved June 5, 2006 from [http://www.ansto.gov.au/ansto/nuclear\\_options\\_paper.pdf](http://www.ansto.gov.au/ansto/nuclear_options_paper.pdf)
- Halliday, D., Resnick, R., & Walker, J. (2008). *Fundamentals of physics extended* (8th ed.). New York: John Wiley & Sons.
- Hore-Lacy, I. (2003). *Nuclear Electricity* (7th ed.). Melbourne: Uranium Information Centre. Retrieved August, 2008 at <http://www.uic.com.au/ne.htm>
- IAEA (2007). *Promoting Nuclear Security: What the IAEA is doing*. Retrieved August, 2008 from <http://www.iaea.org/Publications/Factsheets/English/nuclsecurity.pdf>
- IPCC (2007). *Intergovernmental Panel on Climate Change*. Retrieved April, 2007 from <http://www.ipcc.ch/>
- Maplecroft (2009, September). *Australia overtakes USA as top polluter*. Retrieved September, 2009 from [http://www.maplecroft.com/news/australia\\_overtakes\\_usa\\_as\\_top\\_polluter\\_09.php](http://www.maplecroft.com/news/australia_overtakes_usa_as_top_polluter_09.php)
- Norman, P., Worrall, A. & Hesketh, K. (2007). A new dawn for nuclear power. *Physics World*, **20** (7) 25-30. Bristol: IOP Publishing.
- Nuclear Engineering International Magazine (2004). *Tracking the Technology*. Retrieved April, 2007 from <http://www.neimagazine.com/story.asp?sectioncode=76&storyCode=2024442>
- <http://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0216/r2/br0216r2.pdf>
- NPT Review Conference (2005). *2005 NPT Review Conference*. Retrieved April, 2007 from <http://www.un.org/events/npt2005/index.html>
- Pickett, S. E. (2008). Case Study: Safeguards Implementation at the Rokkasho Reprocessing Plant. In J. E. Doyle (Ed.), *Nuclear Safeguards, security, and non-proliferation*. (pp.165-178). Burlington USA: Butterworth-Heinemann.
- Serway, R.A., & Jewett, J.W. (2008). *Physics for scientists and engineers with modern physics* (7th ed.). Belmont USA: Brooks/Cole-Thomson Learning.
- Swan, G. I. (2008). Nuclear security case study: earthquake in Sichuan Province, China. *Australian Security Magazine*, September/October 2008, pp54-55, Sydney: Yaffa Publishing Group. Retrieved August 2009 from [http://www.securitymanagement.com.au/article.php?action=view&article\\_id=100](http://www.securitymanagement.com.au/article.php?action=view&article_id=100)
- The Australian (2009, August 19). *Bob Hawke in new plug for nuclear waste industry*. Retrieved August 2009 from <http://www.theaustralian.news.com.au/business/story/0,,25950445-36418.00.html>
- The Independent (2008, June 13). *Brown says world needs 1,000 extra nuclear power stations*. Retrieved August, 2008 from <http://www.independent.co.uk/news/uk/home-news/brown-says-world-needs-1000-extra-nuclear-power-stations-846238.html>
- Thornton, S.T., & Rex, A. (2006). *Modern physics for scientists and engineers*. (3rd ed.). Belmont USA: Brooks/Cole-Thompson Learning.
- UN Security Council (2008, March). *Security Council SC/9268*. Retrieved August, 2008 from <http://www.un.org/News/Press/docs/2008/sc9268.doc.htm>
- UN Security Council (2009, September). *Security Council SC/9746*. Retrieved September, 2009 from <http://www.un.org/News/Press/docs/2009/sc9746.doc.htm>

Urenco. (2009). *LES: What we will do*. Retrieved August, 2009 from <http://www.urenc.com/content/150/-What-we-will-do-.aspx>

World Nuclear Association (2009, July). *World Uranium Mining*. Retrieved August, 2009 from <http://www.world-nuclear.org/info/inf23.html>

World Nuclear Association (2009, August). *World Nuclear Power Reactors 2008-2009 and Uranium Requirements*. Retrieved August, 2009 from <http://www.world-nuclear.org/info/reactors.htm>

World Nuclear Association (n.d.). *How it works*. Retrieved April, 2007 from <http://www.world-nuclear.org/how/how.html>

## **COPYRIGHT**

Geoff Swan ©2009. The author/s assign Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. The authors also grant a non-exclusive license to ECU to publish this document in full in the Conference Proceedings. Any other usage is prohibited without the express permission of the authors.

# Firearm Forensics Based on Ballistics Cartridge Case Image Segmentation Using Colour Invariants

Dong Li

secau - Security Research Centre,  
School of Computer and Security Science  
Edith Cowan University

## Abstract

*Ballistics firearm identification based on image processing is of paramount importance in criminal investigation. The efficiency of traditional ballistics imaging system is heavily dependent upon the expertise and experience of end-user. An intelligent ballistics imaging system is highly demanded to address this issues. The segmentation of cartridge case object from the original image is a key step to subsequent process. It is very difficult to segment cartridge case from the original image using traditional threshold based methods due to the shadows or unlimited environments to acquire image. In this paper, we proposed a novel approach based upon the colour invariant and geometrical shape of objects. The experimental results show the proposed method can precisely segment the objects in various images such as heavy shadow, low contrast, uneven illumination etc.*

## Keywords

Ballistics system, firearm identification, image processing

## INTRODUCTION

The analysis of marks on the cartridge case and projectile of a fired bullet is very important to identify the firearm from which the bullet is discharged [1, 2]. When a firearm is loaded and fired, the characteristic marks are produced on the cartridge case and projectile. These marks are significant evidences for identifying the suspicious firearm. Over thirty different features within these marks can be referred as a 'fingerprint' for ballistics recognition [3]. Since each firearm owns its unique toolmarks [4, 5], it is possible to identify both the type and model of a firearm and each individual weapon as effectively as human fingerprint identification.

For ballistics image processing segmentation is the first essential and important step of low level vision. In all these areas, the quality of the final output depends largely on the quality of the segmented output[6]. Conventional algorithms are mainly based upon one of two basic properties of reflective light intensity values, namely discontinuity and similarity[7]. Given that the objects in an image appear lighter (or darker) than the background, one may attempt to segment the image by means of global threshold or local thresholds. A drawback of these approaches is that the result of segmentation is strongly affected by luminance, shadow and noise. In this paper, we proposed a new segmentation algorithm, which based upon the colour invariants and geometrical shape of objects. The colour invariant functions are demonstrated to be invariant to a change in the imaging conditions, such as viewing direction, object's surface orientation and illumination conditions[8]. Therefore this method can overcome the impact of luminance and shadow which is often a difficult task in the traditional pre-treatment of images.

The satisfactory results are obtained using this method in segmentation of cartridge in ballistics images. These images are often acquired across a range of different conditions and usually include shadows. Most background will be removed by using colour invariant properties. But the resulting image still contain some points which belong to the original background which cannot be removed because the RGB values are unstable near the black vertex of the RGB space, where it is undefined[9], while hue is unstable near its singularities at the entire achromatic axis[10]. The remaining points will be removed based on the geometry of cartridge. After these two steps, the cartridge can then be precisely segmented from the image. The method of the algorithm is detailed as follows:

**Step1:** Image acquirement. In order to benefit segmentation of cartridge, a selection of background colour is done firstly. The colour invariant values of background have at least 0.2 differences from the invariant values of the objects which will be segment from the image. Then the original image can be acquired using selected background.

**Step2:** Remove the most background from the original image depend upon colour invariant properties

**Step3:** Remove the rest black shadows which cannot be removed using colour invariant properties because colour invariant properties are unstable near the black vertex of the RGB space.

**Step4:** Search for the range of objects by geometrical shape of objects using Hough transform, then segment the objects base upon the result of Hough transform.

This paper is organized as follows. In Section 2, describes the colour invariant properties, selection of background and image acquirement method, whilst the segmentation algorithm is described in Section 3. Experimental results are presented in Section 4, and in Section 5 conclusions are given.

## IMAGE ACQUIREMENT

### 2.1 Color invariant properties

Firstly, we briefly describe the colour invariant properties employed in our approach. Photometric colour invariants are functions which describe the colour configuration of each image point discounting shadows, and highlights[11]. These features are demonstrated to be invariant to a change in the imaging conditions, such as viewing direction, object’s surface orientation and illumination conditions[8]. Colour invariants features are acquired by RGB[3]. In particular, among the different photometric invariant colour features, as stated in[11], we adopted the  $c_1c_2c_3$  model. The  $c_1c_2c_3$  invariant colour features are defined as follows:

$$C1(x, y) = \arctan \frac{R(x, y)}{\max(G(x, y), B(x, y))}$$

$$C2(x, y) = \arctan \frac{G(x, y)}{\max(R(x, y), B(x, y))}$$

$$C3(x, y) = \arctan \frac{B(x, y)}{\max(R(x, y), G(x, y))}$$

The  $R(x,y),G(x,y),B(x,y)$  representing the red ,green and blue components of a pixel in a image.

Fig. 1 is an example of colour invariant features. There are same background in Point A and B. The difference is point A in light but point B in shadow. Table 1 shows the values of point A and B in two spaces. The invariant colour values have a small change caused by noise but RGB values have a large change.



Fig. 1. Invariant colour features

Table 1 invariant colour and RGB value

point	Invariant color Values			RGB Values		
	$C_1$	$C_2$	$C_3$	R	G	B
A	0.55	1.00	0.54	65	106	62
B	0.54	1.03	0.38	3	5	2

### 2.2 Select color of background

It is not an easy problem to segment cartridges from image initially obtained due to the shadows of cartridges and unequal luminance. The Dong[12] used a ring lights to help to minimize these effects. Yet, such a system still has two major drawbacks. One is that the ring lights depress the contrast density which is very important information for recognition, the other is it has a limited range dependent upon the technician, the lighting as well as other environmental

conditions. However, the segmentation process based on invariant properties can work well on the images acquired without any special conditions.



Fig2. 8 typical samples of cartridge

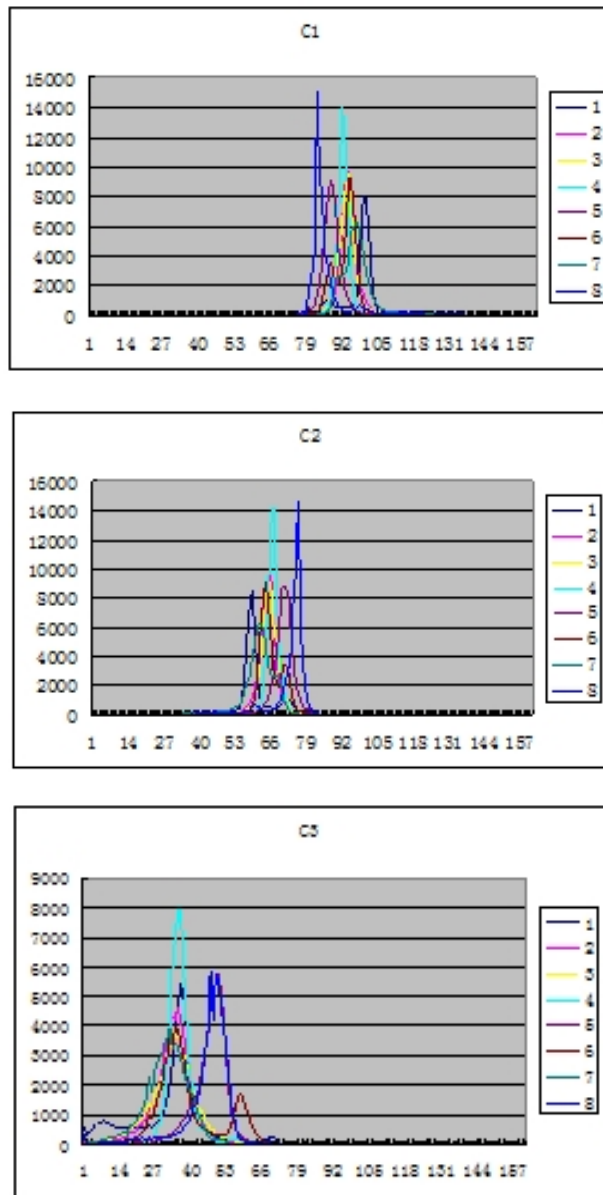


Fig. 3 Values of c1, c2 and c3

In order to use colour invariants, we must select a background and ensure that its colour invariant values do not overlap the cartridge's values. Firstly, we have measured eight familiar types of cartridge. We know that  $\arctan \in [-\pi/2, \pi/2]$ . Moreover, RGB are positive, so  $c_1, c_2, c_3 \in [0, \pi/2]$ . In order to find the range of  $c_1, c_2, c_3$  of cartridge, we select 8 typical images of cartridge [Fig. 2] to compute their values of  $c_1, c_2, c_3$ . The results show in Fig. 3, where, X-axis is the value of  $c_1, c_2$  or  $c_3 \times 100$ , Y-axis is the number of pixels with the same invariant value, and the size of sample images is  $300 \times 300$ . The Fig. 3 shows the values of  $c_1, c_2$  or  $c_3$  are concentrated, and their values are respectively  $C_1 \in [0.71, 1.11], C_2 \in [0.4, 0.80], C_3 \in [0, 0.80]$ . So it's easy to select a background which values of  $c_1, c_2, c_3$  have enough distance with the values of cartridges. Therefore, we set the distance to 0.2, which means the values of  $c_1, c_2, c_3$  in background colour are respectively  $C_1 \in [0, 0.5]$  or  $C_1 \in [1.3, 1.57], C_2 \in [0, 0.2]$  or  $C_2 \in [1.0, 1.57], C_3 \in [1.0, 1.57]$ . According to the range of  $c_1, c_2, c_3$  in background, we search the available background using RGB by computer and get the values are  $R \in [0, 106], G \in [0, 24], B \in [120, 255]$ . The RGB values produced by the same object may change because of differences in input devices, illumination etc. Therefore, we select the middle value of available RGB as the background, which is  $R=54, G=12, B=170$ , their corresponding values of colour invariant properties is  $c_1=0.31, c_2=0.07, c_3=1.26$ . The colour with  $R=54, G=12, B=170$  is near to purple, so we select a purple as a background. And it is proved that the purple is a good background to segment cartridge by extensive experiments.

### 2.3 Image acquirement

Image acquirement is a simple step and requires no other condition except using a background such as that described in section 2.2. Then the image can be acquired using a digital camera or a video camera.

## IMAGE SEGMENTATION

A novel method to segment the cartridge based on the colour invariant features and geometry is employed. This method included three steps. 1) Removing background using colour invariant; 2) Removing black shadow; 3) search for the range of cartridge by geometry. A detailed description of the three steps is given in the following sections.

### 3.1 Removing background

In order to remove the background, we must know the values of  $c_1, c_2, c_3$  in that background. The 4 corners in each image are the background due to the circular cartridge, so we get a small image with  $10 \times 10$  in each corner of the image (shows in Fig. 1 with a white rectangle in each corner). Thus, we obtain 4 small images, and compute the average values of  $c_1, c_2, c_3$  in all 4 small images, and save them in variables  $rc_1, rc_2$  and  $rc_3$  as the reference values of background. Then all pixels in the image are scanned and set to white if the differences between the invariant value of pixel and the reference value are all more than 0.2. Benefiting from the special background colour, the differences between the invariant value of the cartridge and the reference value are generally more than 0.2. Thus the operation cannot modify the value of cartridge. Fig.4 (a) is a result after this operation from Fig. 1.



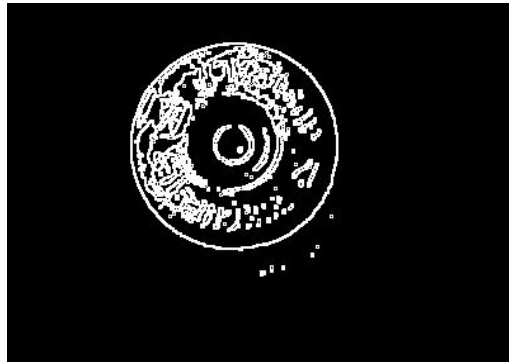
(a)



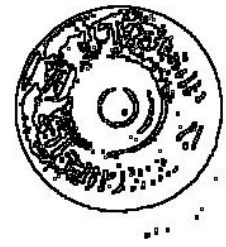
(b)



(c)



(d)



(e)



(f)

Fig. 4 (a) Remove background using colour invariant features  
 (b) Remove black point whose R+G+B value is below 30  
 (c) Binary image using threshold value 255  
 (d) Sobel filter of (c)  
 (e) Binary image of (d)  
 (f) Segmented cartridge using fitting circle

### 3.2 Removing black shadows

Comparing the Fig. 1 and Fig. 4(a), we find the most background colour has been removed. However, it still possesses some pixels which belong to the background which cannot be removed because the RGB values are unstable near the black vertex of the RGB space, where it is undefined[13]. Therefore, the pixels give rise to unstable invariant features values in presence of noise[10]. Otha [12] thinks that the colour invariant properties become unstable and meaningless when R+G+B value is less than 30. So we extracted those pixels whose R+G+B value is below 30 and which are also verified in a wide range of test images that these regions belong to shadows. Therefore we set those pixels to white. After this operation, we obtain the image Fig 4(b) where the black pixels have been removed.

### 3.3 Search for the range of cartridge by geometry

Now, good cartridge images are obtained, but they still have some background pixels, and the borders of cartridge are not smooth [Fig.4 (b)]. Moreover, some pixels of cartridge also are removed because its invariant values fall in removed window. In order to resolve this issue, we use the prior knowledge. It is well know the cartridge is a circle, so we segment the cartridge fitting it into a circle. The method is as follows:

- 1) Firstly we bifurcate the image [Fig.4 (b)] by setting the pixels to black if its RGB values less 255 whilst the remaining pixels are set to white. The aim of this operation is to change the cartridge into black and the background into the white. The best result of this operation is a solid black disc on a white background because such a solid black disc is very useful in detecting the circle of the cartridge. The Fig.4(c) shows the image after this operation.

In Fig.4(c), we can see the black edge form a circle which is just the edge of cartridge. So if we can detect the circle, the cartridge will be segment precisely. It is well know Hough transform is a popular algorithm to detect circle. But the computational cost is very large if the Hough transform is directly undertaken using image [Fig.4 (c)], because the number interesting points, the black pixels, is also very large. So we perform the following two steps to reduce the computational cost of the Hough transform. Firstly, the Sobel filter is applied to produce image [Fig.4 (c)] and also obtain the edge image [Fig.4 (d)]. Then image is binarized [Fig.4 (d)] using Otsu algorithm[9] and the image [Fig.4 (e)] obtained. Now the number of interesting pixels is much less than before, so the amount computation required is also greatly reduced. It should be noted that if the image [Fig.4 (c)] is a solid disc, the image [Fig.4 (e)] will have the least black pixels resulting in the least computational cost of Hough transform.

- 2) Detect the circle in [Fig.4 (e)] using Hough transform. The equation of circle is  $(x-a)^2+(y-b)^2=r^2$ , This familiar equation can be changed into the form  $b = y \pm \sqrt{r^2 - (x - a)^2}$ . So the key to reduce the computational of detecting a circle is to reduce the range of parameters a, b, and r. The steps of setting their range are as following:

I ) Making sure the rectangle contains the points where the circle exists. It is easy to make sure the up left coordinates (LeftX,LeftY) and the bottom right coordinates (BottomX,BottomY). The Fig. 5 shows the rectangle.

II) Once the rectangle is confirmed, the parameter  $r$  can be confirmed in the following way: the maximum  $r \maxR = \min(\text{BottomX} - \text{LeftX}, \text{BottomY} - \text{LeftY}) / 2$  and the minimum  $r \minR = \min(\text{BottomX} - \text{LeftX}, \text{BottomY} - \text{LeftY}) / 3$ . The  $\minR$  is an heuristic value obtained by extensive experiments.

III) Now we can discover the range of  $a$  and  $b$  easily. Minimum  $a \minA = \text{LeftX} + \minR$  and maximum  $a \maxA = \text{BottomX} - \minR$ . Correspondingly we can also discover the values of Minimum  $b \minB = \text{LeftY} + \minR$  and maximum  $b \maxB = \text{BottomY} - \minR$ .

The three steps mentioned above greatly reduce the range of parameters  $a$ ,  $b$  and  $r$ , and so the computation overhead of Hough transform is also greatly reduced.

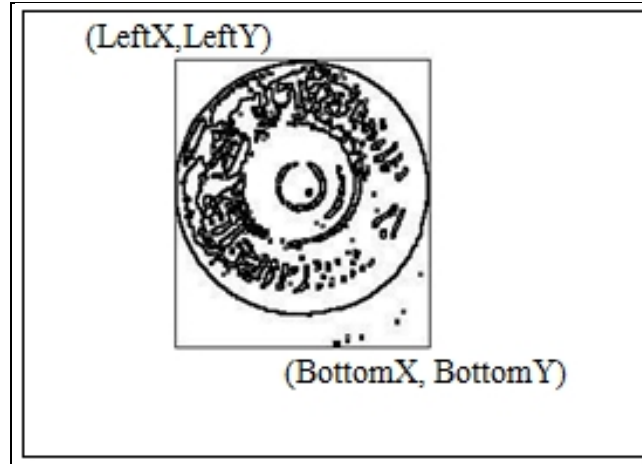


Fig. 5 The Hough Transformed Image

- 3) Set each cell in accumulator  $A(a,b,r)$  to 0. Then, for each black point  $(x,y)$  in Fig. 4(e), we let the  $r$ ,  $a$  equal each of the allowed values, and compute the corresponding  $b$  value using the equation  $b = y \pm \sqrt{r^2 - (x - a)^2}$ . The  $b$  values are rounded off to the nearest integer. If  $b \in (\minB, \maxB)$ , then we let  $A(a,b,r) = A(a,b,r) + 1$ . At the end of the procedure, a value of  $A(a,b,r)$  means that the number of black points lie on a circle  $(x-a)^2 + (y-b)^2 = r^2$ . We can see that the value of  $a,b,r$  in the cell with maximum value in accumulator  $A(a,b,r)$  is the value of the circle which is the edge between the cartridge and the background. (i.e. in [Fig. 4 (e)],  $a=178$ ,  $b=113$ ,  $r=81$ ). Thus, we can extract the circular region of cartridge which coordinates of circle centre is  $(a,b)$  and radius is  $r$  from the original image [Fig. 1]. The image [Fig.4 (f)] is the result of segmentation.

## EXPERIMENTAL RESULTS

### 1.1 Test set

In order to test the proposed algorithm, an experimental database was constructed. Which contained 35 cartridges, and each cartridge had 3 images acquired in different environments: outdoor, indoor, and using a single light source. The Fig. 6A shows images obtained respectively from these three different environments. The image size is given in pixels. Basically, the door image has no shadow, and indoor image has some light shadow, whilst the single light source image has heavy shadowing.

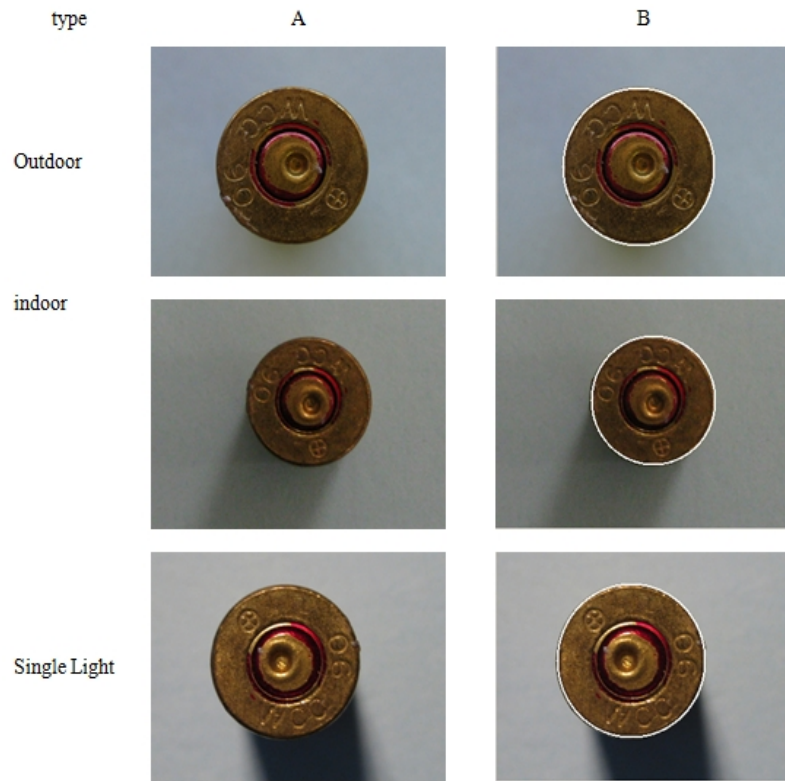


Fig 6 Cartridge segmentation results.  
A: Original image  
B: Detected cartridge (within white circle)

### 1.2 Cartridge segmentation results

The 105 640×480 images in our database were segmented. All cartridges could be segmented precisely. Figure 6 shows the results of the proposed algorithm for one cartridge in 3 environments. The original images (Fig. 6A) and the detected cartridges on the original image (Fig. 6B) are displayed. In order to display the detected precision, we do not segment the cartridge from the original image, but show the detected region by a white circle. From Fig.6B, we can see the cartridges are precisely detected by the proposed algorithm. It takes about 1.2s to segment object from the source image with 640\*480 pixels on PC(CPU: Intel Pentium4 2GHz, RAM: 1GB).

## CONCLUSION

In this paper, we described an efficient method for segmenting cartridge images. This proposed method is based on colour invariant properties as well as geometry. The proposed approach was demonstrated through its application to a number of test images obtained under three common different forms of illumination. This method has no special limitations in respect to the image input environment except that of a designated background. A method of reducing computational overhead was also presented.

Firearm identification aims to provide a link between the suspect firearm and the forensic ballistics specimens based on the depressions, scratches and markings on the specimens of cartridge cases and projectiles. These various marks are called ‘toolmark’ and it is thought that the toolmark is unique to itself. In this regard, it is possible to identify the suspect firearm by toolmark left on ballistics specimens with advanced image processing technologies.

### Acknowledgement

The ballistics specimens were provided by Australia Police. Mr Z. Huang, as a visiting fellow at ECU, helped with digital image acquisition.

## REFERENCES

- Dongguang Li, "Ballistics Projectile Image Analysis for Firearm Identification," *IEEE Transaction on Image Processing*, vol. 15, pp. 2857-2865, 2006.
- R. Saferstein (ED), "Forensic Science Handbook," *Volume 2. Englewood Cliffs: Prentice Hall*, 1988.
- G.Burrard, "Identification of Firearms and Forensic Ballistics," *London, U.K:Herbert Jenkins*, 1951.
- A. Biasotti and J. Murdock, "Criteria for identification or State of the Art of Firearm and Toolmark Identification," *AFTE Journal*, vol. 16, pp. 16-34, 1984.
- A. Schwartz, "A Systemic Challenge to the Reliability and Admissibility of Firearms and Toolmark Identification," *The Columbia Science and Technology Law Review*, vol. VI, pp. 1-42, 2005.
- Pal, N.R. and S.K. Pal, *A review on image segmentation techniques*. Pattern Recognition, 1993. 26(9): p. 1277-1294.
- Rafael C. Gonzalez, R.E.W., *Digital Image Processing (Third Edition)*. Pearson Education.Inc, 2008.
- Gevers, T., *Color-based object recognition*. Pattern Recognition, 1999. 32(3): p. 453-464.
- J. Kender, *Saturation, Hue, and Normalized colors: Calculation, Digitization Effects, and Use*. Tech. Rep., Carnegie-Mellon University, 1976.
- Gevers, T., *Classifying color edges in video into shadow-geometry, highlight, or material transitions*. IEEE Transactions on Multimedia, 2003. 5(2): p. 237-243.
- Elena Salvador, A.C., Touradj Ebrahimi,, *Cast shadow segmentation using invariant color features*. Computer Vision and Image Understanding 95 (2004) 2004: p. 238-259.
- Ohta, Y., *Color Information For region Segmentation*. Computer Graphics and Image Processing, 1980. 13(3): p. 222-241.
- Otsu, N., *Threshold Selection Method From Gray-Level Histograms*. IEEE Transactions On Systems Man and Cybernetics, 1979. 9(1): p. 62-66.

## COPYRIGHT

Dong Li ©2009. The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors