

Forensic Computing Theory & Practice: Towards developing a methodology for a standardised approach to Computer misuse

Mathew Hannan¹
Sandra Frings²
Vlasti Broucek³
Dr Paul Turner³

¹ School of Accounting and Information Systems
University of South Australia
e-mail: mathew.hannan@unisa.edu.au

² Fraunhofer Institut fuer Arbeitswirtschaft und
Organisation Competence Center Software-Management
Stuttgart, Germany
e-mail: Sandra.Frings@iao.fhg.de

³ School of Information Systems
University of Tasmania
e-mail: Vlasti.Broucek@utas.edu.au
e-mail: Paul.Turner@utas.edu.au

Abstract

The increasing risk and incidence of computer misuse has raised awareness in the public and private sectors of the need to develop defensive and offensive responses. There is now widespread recognition of the importance of specialised forensic computing investigation (FCI) teams able to operate across conventional boundaries of law enforcement and national defence. More specifically, recent research on Australian FCI teams has revealed the critical role of investigative skills alongside digital evidence acquisition and presentation competences. At the level of practice these investigative skills extend beyond a methodical approach, to include case management, critical thinking and sensitivity to the corroborative importance of non-digital evidence. This paper considers the implications of these practical insights for forensic computing theory and presents a matrix for classifying behaviours and types of computer misuse. It also examines the European CTOSE methodology and reflects on how it is re-contextualised by these insights derived from FCI practice. It is anticipated that this paper will contribute towards the development of a standardised and comprehensive forensic approach to computer misuse.

Keywords

Forensic Computing, investigation, e-security, e-crime, criminal behaviour, computer misuse, digital evidence.

INTRODUCTION:

The diffusion of information and communication technologies (ICT) throughout government, business and society has led to new opportunities, risks and challenges for legal, technical and social structures. A major factor in these risks and challenges are the numerous ways that individuals and/or groups can use ICTs to engage in inappropriate, criminal or other illegal behaviour. More specifically, the increased risk and incidence of criminal, illegal or inappropriate computer and on-line behaviours has heightened awareness in the public and private sectors of the need to develop defensive and offensive responses (McKemmish 1999; ACPR 2000; ACPR 2001; Broucek & Turner 2001).

Although detailed figures on the scale of computer misuse are difficult to obtain, the problem of computer misuse is already very significant. For example, by the year 2000 approximately 70% of US corporations had reported e-crime incidents up from 40% in 1999 at an estimated cost of around \$US266 million in 2000 (AFP, 2001). In Australia a similar trend has been observed. The Australian Computer Emergency Response Team (AusCERT) recorded similar increases in e-crime response requests from Australian organisations over the period 1998 to 2000 and AusCERT's most recent Computer Crime and Security Survey reported that 42% of respondents had experienced one or more significant attacks that had harmed the integrity, confidentiality or availability of network data or systems. Other trends identified by AusCERT were:

- Greater occurrence of externally-sourced harmful attacks

- Financial losses had doubled over the last year (\$12 million in 2003, compared with \$6 million in 2002) due to computer attacks which harmed the confidentiality, integrity or availability of network data or systems
- Financial fraud, laptop theft and virus, worm and Trojan infections as being the largest source of computer crime losses
- 22% of organizations surveyed experienced more than ten computer security incidents.

(Source: AusCERT, 2003)

While the reported incidence of computer misuse is clearly on an upward trend, there remains a lack of comprehensive data on the nature, level and frequency of these behaviours or on their consequences. This is further compounded by non-reporting and non-detection of computer misuse and e-crime (ACPR 2000; Etter 2001b). In this context, it is hardly surprising that public and private sector organisations have sought ways to respond. These responses have included increased security precautions, monitoring, education and deterrence. There has also been recognition that when computer misuse is detected it is critical to investigate both the effects of the misuse and to collect and analyse evidence to support future actions that may involve criminal or civil prosecution, organisational censure or dismissal. As a consequence, many organisations have established forensic computing investigation (FCI) teams. However, the dynamic and multi-faceted nature of computer misuse has meant that these teams face challenging decisions over the nature, level and types of skills and competences that they should contain (Hannan & Turner, 2003a).

Significantly, recent Australian research conducted into the skills and practices of 21 FCI teams has revealed the critical role of investigative skills alongside digital evidence acquisition and presentation competences. At the level of practice these investigative skills extend beyond a methodical approach to the investigation to include case management, critical thinking and sensitivity to the corroborative importance of non-digital evidence (Hannan & Turner, 2003a).

As knowledge and experience in conducting forensic computing investigations grows, it is imperative that these practical insights are used to expand and inform forensic computing theory. In this context, this paper considers the implications of these practical insights for forensic computing theory and presents a matrix for classifying types of computer misuse. It also examines the European CTOSE evidence acquisition methodology and reflects on how it is re-contextualised by these insights from FCI practice. It is anticipated that this paper will contribute towards the development of a standardised and comprehensive forensic approach to computer misuse.

RE-THINKING FORENSIC COMPUTING: A PRACTICE-BASED PERSPECTIVE

At the level of theory, accurately defining forensic computing has proven to be a difficult task. Two of the most commonly accepted definitions used by academics and practitioners illustrate the different technical or legal emphasizes that exist:

McKemmish (1999) has defined forensic computing as:

"The process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable"

(McKemmish, 1999:1)

Farmer and Venema (1999) have defined forensic computing as:

"Gathering and analysing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system"

(Farmer & Venema, 1999)

From a technical perspective, system advances in intrusion detection, network monitoring and identification of denial of services attacks are well documented and subject to on-going research and development. However, these technical systems are not currently designed to collect forensic data and administrators are also generally unfamiliar with the processes for evidence acquisition. From a legal perspective, legal regimes are struggling to address the challenges posed by criminal, illegal and inappropriate computer behaviours. These challenges include both conceptual problems of definition and problems of legal jurisdiction. Most legal professionals have a limited understanding of technical advances and lack confidence in the ability of technical specialists to produce evidence that will be admissible in a court of law (Broucek & Turner, 2002).

Significantly, recent trends observed in FCI practice suggest that whilst both of the above definitions have merit they need to be expanded to encapsulate the role of investigative skills and the emergence of pro-active as well as post-mortem forensic computing activities (Hannan & Turner 2003a, 2003b). Noticeably, FCI teams are no longer restricted to law enforcement or defence organisations and have emerged in numerous industry sectors that traditionally have had little contact with criminal investigation. Indeed, much of the work of these new FCI teams involves investigations for civil proceedings or internal organisational actions. This highlights that many forensic investigations now occurring will often not be subjected to examination in the legal system. It also emerges from FCI practice that distinctions are acknowledged between pro-active monitoring/intelligence gathering and post-mortem investigations.

While at a theoretical level every forensic investigation should follow the same procedures of care and attention to not contaminating evidence, where FCI teams are engaged in investigations that will have no legal presentation, 'short cuts' are often deployed. This may be the case when the investigation team knows that they can achieve a specific outcome without the scrutiny that would be placed upon the evidence in legal proceedings. FCI teams also exhibit sensitivity to the corroborative importance of non-digital evidence and often utilise this in conjunction with other forensic techniques in responding to the challenges of computer misuse. In organisational settings, existing policies, practices and procedures governing inappropriate computer behaviour may allow for discretion on the behalf of the investigative team. In the context of these practice-based insights, an alternative definition of forensic computing could be as follows:

"Processes or procedures involving monitoring, collection, analysis and presentation of digital evidence as part of 'a priori' or 'post-mortem' investigations of computer misuse".

Nevertheless, while in practice FCI teams may use their discretion, there remains a danger that in certain circumstances and in response to certain types of computer misuse not following strict principles in acquiring digital evidence may lead to its inadmissibility in any subsequent legal or criminal investigations undertaken. In this context, it is useful to clearly identify the range of criminal, illegal and inappropriate behaviours and types of computer misuse that exist. The next section presents a matrix of these behaviours and types of misuse which it is anticipated will assist academics and practitioners in considering forensic computing responses and how best to calibrate them to the needs of particular investigations.

DEVELOPING A MATRIX OF BEHAVIOURS AND TYPES OF COMPUTER MISUSE

As with the investigation of traditional societal misconduct, the need to classify the type of misconduct early in the investigation is of paramount importance to identify the type of forensic evidence and the best methods for its collection, analysis and presentation. The matrix of criminal, illegal and inappropriate computer behaviour (figure 1.) provides a tool for rapidly identifying types of computer misuse and the level of seriousness of its associated behaviour. It is envisaged that the matrix can contribute to the development of a methodology for a standardised approach to computer misuse.

Criminal, Illegal and Inappropriate Computer Behaviour

The development of this matrix is based upon the identification of behaviours produced by Broucek and Turner (2001). The behaviours identified are: Criminal, illegal or inappropriate.

In examining this classification of behaviour it can be observed that they can be ranked in a descending order of severity. Criminal law reflects those behaviours that have been identified as being unacceptable to society at large and mostly relate to people and property. Civil laws have developed to provide protection for individuals and organisations in the areas of commerce, trade and the employment relationship. Inappropriate acts are acts that are determined by transgression of the various boundaries set by social, organisational or individual norms of behaviour.

Significantly, both criminal and illegal behaviours are defined by the jurisdiction in which legal proceedings are enacted. Although, in the realm of forensic computing investigations the determination of where computer misuse occurs and which legal jurisdiction has precedence or is most appropriate for proceedings is often itself fraught with difficulties. In relation to the term inappropriate behaviour it is clear that this can be used to refer to acts committed by the use of, or involving, a computer or electronic device that contravene particular norms, codes or principles of behaviour in specific social, organizational or individual circumstances. In other words, inappropriate behaviour is tied to specific circumstances (Social, Spatial, Temporal) such that what may be acceptable within one domain may be entirely inappropriate in another, and that these circumstances are dynamic and change.

Types of Computer Misuse

The behavioural aspects of the matrix identified above can now be cross-referenced with types of computer misuse. In order for an act to occur or behaviour to be exhibited in the digital environment digital data must be created and/or transferred. This data creation and/or transfer occurs as follows:

- Human to digital device
- Digital device to digital device
- Digital device to Human

In this context, computer misuse can be broadly divided into two categories. The first category involves the misuse arising from the generation, collection, storage, manipulation or distribution of data that itself constitutes a criminal, illegal or inappropriate behaviour. In this category it is the nature of the content of the data/information (whether encrypted or not) that constitutes the misuse with the electronic means by which it is being delivered being merely a transmission mechanism. For example, child pornography, software viruses, worms etc. In this category, the FCI team would seek to prove that the delivery was intentional and the content of the transmission was not altered from the sender to the recipient. It would be the judgement of the adjudicating senior manager, civil judge, or criminal judge (or jury) as to whether the nature of the content of the transmission constituted criminal, illegal or inappropriate behaviour.

The second category involves misuse arising from the actions of the user deploying digital devices. This category is distinctly different from the first in that the information being generated, collected, stored, manipulated or distributed does not in itself constitute a criminal, illegal or inappropriate behaviour. In this category it is rather the actions and intentions of the user and the nature of data/information transfer that may constitute the criminal, illegal or inappropriate behaviour. For example, denial of services attacks, hacking etc. In this category, the FCI team would be required to prove that the information transferred was intended to result in a specific criminal, illegal or inappropriate result. Or that a reasonable person would believe that such an outcome was likely given the type of behaviour undertaken. The FCI team would be required to prove this and the intentionality of the individual under investigation.

While this matrix (Figure 1) provides a simplistic division of behaviours and types of computer misuse, it is clear that the determination of how to categorise particular events is partly determined by whether the data and/or actions are captured for examination prior to, during, or after the event. However, as a heuristic device for considering computer misuse behaviours it is anticipated that this matrix will prove useful for conceptualising behaviours and type of misuse for investigation and analysis by practitioners and academics.

Figure 1 provides a diagrammatic representation of the matrix presenting both the behavioural aspects and the computer misuse categories of the matrix.

		COMPUTER MISUSE	
		Category 1	Category 2
BEHAVIOUR	Criminal		
	Illegal		
	Inappropriate		

Figure 1. A Matrix of Criminal, Illegal and Inappropriate Computer Behaviour

THE EUROPEAN CTOSE METHODOLOGY AND REFLECTIONS FROM FORENSIC PRACTICE

The above discussion has highlighted that there exist different emphasizes between the foci of forensic computing theory and current practice. One recent attempt to address these issues has been the European Union (EU) funded project 'Cyber Tools On-Line Search for Evidence (CTOSE)'. CTOSE has developed a methodology that aims to provide a consistent approach for identifying, preserving, analysing and presenting digital evidence.

Background and motivation

A major motivation for the establishment of the CTOSE project was recognition that in most companies IT security management still often consists of purely technical measures in the area of prevention and detection of IT incidents. In these circumstances, the first priority is always the prevention of further incidents and the elimination of the technology vulnerability of the technology, while little attention is usually given to forensic investigation to find out what happened or trace the perpetrators. Even where investigations occur there is often a problem of a lack of experience or knowledge of how to proceed correctly both from a technical and/or legal perspective. Alternatively, companies are reluctant to instigate investigations because of the implications of delays in the operational running of the business or they fear damage to their company reputation if the incident becomes public.

The solution

To address these issues and improve the ability of companies to respond to computer misuse incidents the CTOSE project began by developing a reference process resembling organisational, technical and legal guidelines on how a company should proceed when computer misuse occurs. The focus of the model is on the acquisition of digital evidence and on how it is to be collected, conserved and analysed in a manner that will be legally admissible should court proceedings be instigated. Figure 2 illustrates how this reference model links to a detailed examination of technical, legal and presentational requirements, which in-turn link to the project software demonstrator.

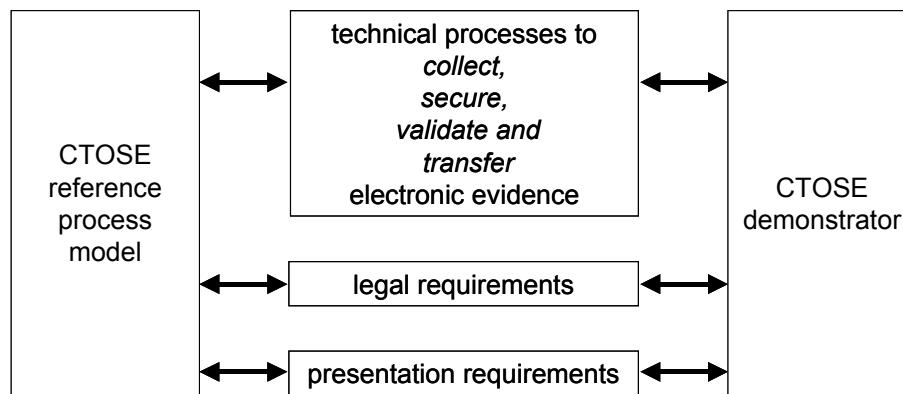


Figure 2. CTOSE Project

The reference process model is composed of five phases: preparation, running, assessment, investigation and learning phases. It articulates the flow of actions and decisions that have to be considered or executed in the case of an investigation of computer misuse. Moreover, additional information, (including: roles and their necessary skills, checklists, references to documents and tools, and legal advice) to support the action or decision in each step (see Figure 3). In this way a user can, for example, consult a checklist, prior to reporting an IT incident, which covers what technical information about the incident law enforcement agencies may require from the person involved. This should result in optimising communication between the two parties.

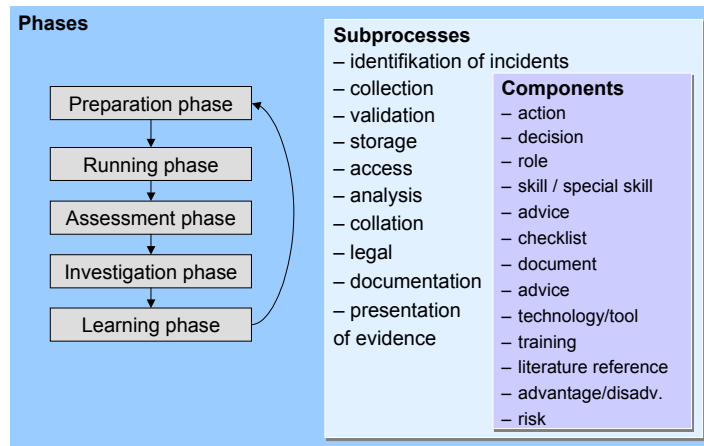


Figure 3. CTOSE Phases of response.

Significantly, the CTOSE project emphasizes the preparation phase, also referred to as ‘Forensic Readiness’, because IT security measures critical to the whole process are defined and implemented in this phase. For example, the implementation of a firewall or an intrusion detection system.

The software prototypes

As a consequence of the complexity of the process reference model it was decided that the CTOSE project would develop an electronic version. This version is called the Cyber Crime Advisory Tool (C*CAT) and involves a database connected to a database administration tool (written in JAVA) containing all actions, decisions, relationships (sequence of flow charts) and all additional information. The architecture of C*CAT is presented in Figure 4.

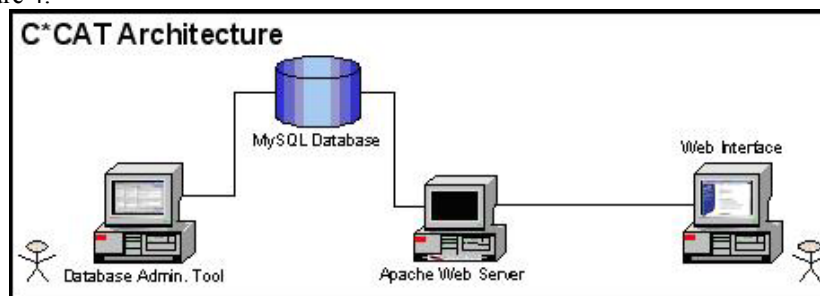


Figure 4. C*CAT Architecture

Examples of the update function of some components of the database administration tool are shown in Figure 5.

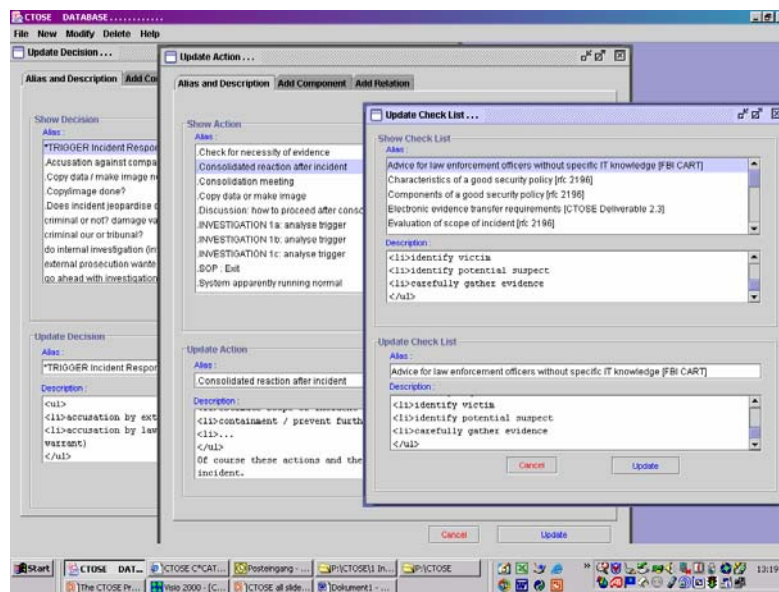


Figure 5. Update Functions of C*CAT.

The Web front end of C*CAT (see Figures 6 & 7) connected via an Apache Web server to the database is the interface between the information to be processed and the people involved in investigating a computer misuse incident.

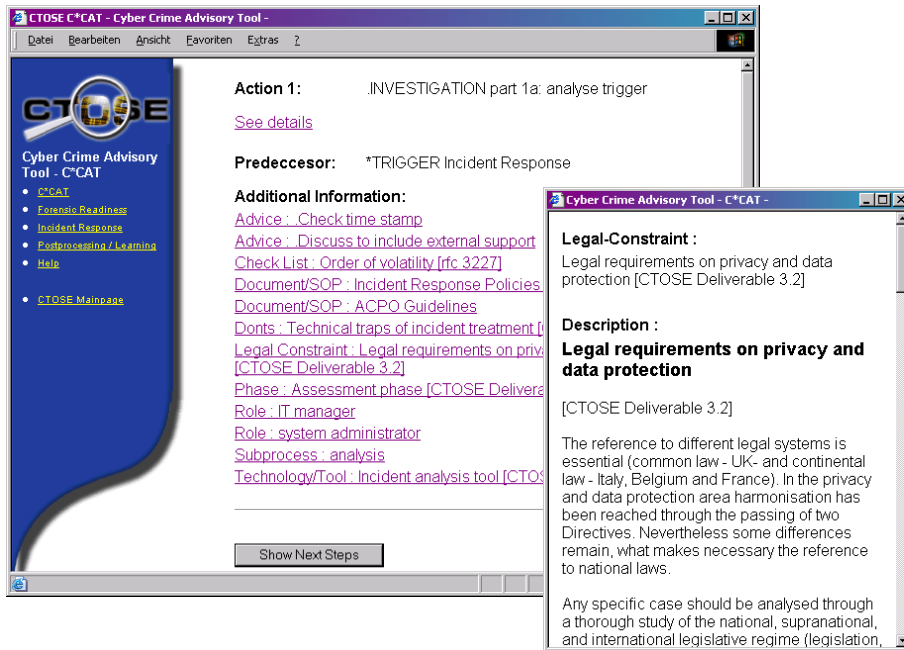


Figure 6. Web front end of C*CAT

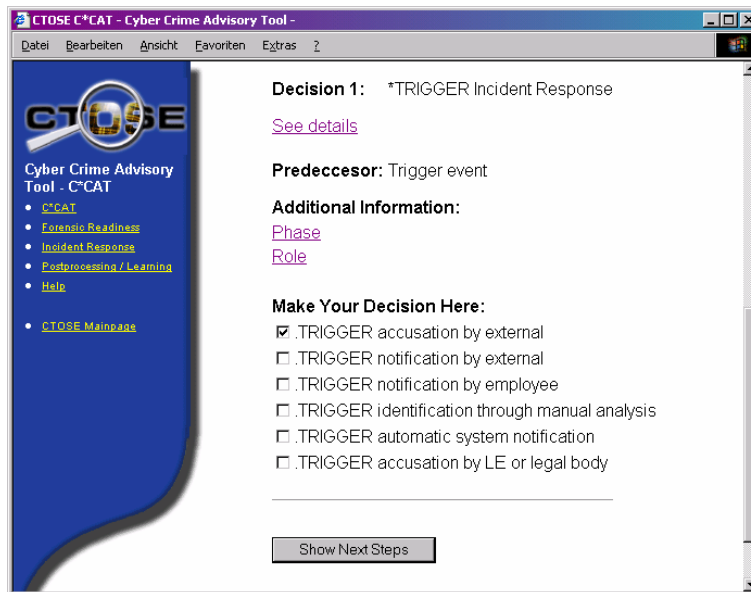


Figure 7. Web front end of C*CAT

From evaluation of C*CAT it is clear that it is easy to use and allows users to define the situation (by selection among different choices). Following this phase C*CAT presents the necessary actions and decisions that should be taken. In each case the user is able to ask for more advice and guidance. Since the integrity of the chain of custody is critical, following correct procedures is of vital importance. At the end of the process, the user will be able to give feedback concerning the usage of the model to further improve its operation and utility.

The future aim of CTOSE is to refine and improve the methodology and distribute it as widely as possible. As part of these activities the CTOSE project has developed a simulation environment (CTOSE Demonstrator) as an educational awareness and validation tool. The demonstrator describes the process model using several different scenarios. Each scenario provides the user with a clear and understandable way to proceed with do's and don'ts when handling digital evidence for each phase. The project anticipates that the widespread utilization

Hannan, Frings, Broucek, Turner (Paper #21)

of the CTOSE methodology will assist companies in being able to recover more rapidly from computer misuse incidents and improve their ability to conduct computer forensic investigations (Frings, Stanistic-Petrovic & Urry, 2003).

From the above discussion it is clear that the CTOSE project has made a very significant contribution to developing a methodology for a standardized approach to computer misuse. However, previous insights from FCI practice also re-contextualise the CTOSE project by drawing attention to the critical role of the 'forensic readiness' phase and how in practice this phase already involves pro-active monitoring and analysis of digital evidence. It is also clear that the methodology may provide firms with a false sense of security when conducting investigations. From FCI practice it is readily acknowledged that digital evidence can be created easily and so therefore must be treated with care in case it has been tampered with (Broucek & Turner, 2003). Perhaps more significantly there is also a danger of creating an artificial separation between digital evidence and other types of evidence of computer misuse. From a practice perspective sensitivity to the corroborative significance of non-digital evidence can often provide important indications of criminal, illegal or inappropriate computer behaviours. Above all, there remains the problem of identifying behaviours and types of computer in the first place and it is to be hoped that the matrix and insights from FCI practice will assist moving towards the development of a standardized approach to computer misuse.

CONCLUSION

This paper has aimed to make a contribution towards developing a methodology for a standardized approach to computer misuse. By drawing on practical insights from current FCI practice a more holistic conceptualisation of forensic investigation has been presented. This conceptualisation involves recognition of 'a priori' as well as post-mortem activities, the critical role of investigative skills and the need to be able to easily identify behaviours and types of computer misuse.

By drawing on the significant work that has already been done in Europe within the CTOSE project it is hoped that the practical insights identified will contribute to refining this methodology and alerting academics and practitioners of the need to remain vigilant in calibrating responses that are adequate to the address dynamic and multi-faceted nature of issues in the forensic computing domain.

REFERENCES

- ABS (2001). Census of Population and Housing, Australian Bureau of Statistics. 2001.
- Broucek, V & Turner, P (2001) Forensic Computing: Developing a Conceptual Approach in the era of Information Warfare, Journal of Information Warfare, Volume1, Issue 2 (ISSN1445-3312).
- Broucek, V & Turner, P (2002) Bridging the Divide: Raising Awareness of Forensic Issues amongst Systems Administrators (2002) 3rd International SANE Conference 27-31 May, 2002 Maastricht, the Netherlands (www.nluug.nl/events/sane2002/)
- Broucek, V & Turner, P (2003) A Forensic Computing perspective on the need for improved user education for information systems security management, in R. Azari (Ed.), Current Security Management & Ethical Issues of Information Technology. Hershey, PA 17033-1117, USA: IGP/INFOSCI/IRM Press (ISBN 1-931-777-43-8).
- Farmer, D., & Venema, W. (1999). Internet Security Auditing Class Handouts, [www]. Available: <http://www.porcupine.org/auditing/> [2001, 10 January 2001].
- Frings, S., Stanistic-Petrovic, M., & Urry, R. (2003). Holistic Approach for Processing Electronic Evidence Related to High-Tech Crime and Severe Disputed Electronic Transactions: Cyber Crime Advisory Tool - C*CAT. Paper presented at the EICAR 2003, Copenhagen, Denmark.
- Hannan, M. & Turner, P. (2003a). "Beyond the Matrix: Research on Competence among Australian Forensic Computing Investigation Teams" Proceedings of the 2nd European Conference on Information Warfare and Security, June 30 – July 1, 2003. Reading:U.K.
- Hannan, M. & Turner, P. (2003). "Australian Forensic Computing Investigation Teams: Research on Competence" Proceedings of The Seventh Pacific-Asia Conference on Information Systems, July 10 – July 13, 2003. Adelaide: Australia.
- McKemmish, R. (1999). What is Forensic Computing? Trends and Issues in Crime and Criminal Justice (118).

COPYRIGHT

[Hannan, Frings, Broucek, Turner] © 2003. The authors assign to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to ACIS to publish this document in full in the Conference Papers and Proceedings. Those 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.