Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:26
Received 6 June 2003

Mr J Keelty APM
Commissioner
Australian Federal Police
GPO Box 401
CANBERRA ACT 2601
☎02 6275 7611   🖹02 6275 7766
E-mail:

PARLIAMENTARY JOINT COMMITTEE ON THE AUSTRALIAN CRIME COMMISSION

CYBERCRIME INQUIRY

Submission by the:

Australian Federal Police / Australian High Tech Crime Centre

May 2003

Table of Contents

Parliamentary Joint Committee on High Tech Crime for the Australian Crime Commission

Submission by the: Australian Federal Police / Australian High Tech Crime Centre

1. Introduction

This submission to the Parliamentary Joint Committee (PJC) represents both the Australian Federal Police (AFP) and the Australian High Tech Crime Centre (AHTCC). The AHTCC is a national police body reflecting the interests of all Commonwealth, State and Territory police agencies on high tech crime matters. The AHTCC is hosted by the AFP in Canberra.

The structure and functions of the AHTCC are in the process of being finalised, with the current staffing and operations being that of the AFP High Tech Crime Team (HTCT). As such, this submission largely reflects the current operations of the AFP HTCT. In the future, it is envisioned that separate submissions by the AFP and the AHTCC will be provided to the PJC.

2. High Tech Crime

Electronic crime or 'e-crime' has been defined as crime where the computer is the tool, the target, or the repository of information about the crime. Given the prevalence of technology and computer devices in Australian society, almost any type of crime could be considered 'e-crime'. Therefore, the AFP and AHTCC have chosen to use the term 'high tech' crime to more ably describe the type of criminality that should be addressed in a nationally coordinated manner.

High tech crimes are typically multi-jurisdictional and effective prevention and response requires national and international coordination. High tech crime includes both:

1. those crimes committed directly against computers and communications systems such as computer hacking, denial-of-service, or malicious software writing and distribution (e.g. viruses, worms, Trojans), as defined in the *Commonwealth Cybercrime Act 2001*; and

2. a range of more 'traditional' crime types which are facilitated by technology. These include child sexual exploitation, illicit drug importation, fraud, extortion, industrial espionage, money laundering and terrorism. These crimes can be considered 'high tech' where the activity is substantially dependant on, or facilitated by technology.

This view of high tech crime is consistent with the National Hi-Tech Crime Unit (NHTCU) in the United Kingdom which defines high tech crime as "new crime - new tools, old crime - new tools" (www.nhtcu.org). The NHTCU was studied as a model for the creation of the AHTCC.

The Internet

The economic and societal benefits achieved through the use of the Internet are well documented. Governments around the world are actively pursuing electronic commerce and encouraging the uptake of Internet enabled technologies. However there are attributes of the Internet which are also attractive to criminals.

In particular, the Internet:

- provides global reach to a large number of potential victims and criminal partners;
- increases the perception of anonymity;
- diversifies and diffuses communications and transactions; and
- causes evidence of crime to resides in systems, jurisdictions and countries removed from the origin of the crime and/or the victim.

AFP Operating Environment

The ability of law enforcement agencies such as the AHTCC to effectively operate in the electronic environment requires a strong cooperative framework both nationally and internationally. The AFP is represented on a number of groups that assist in ensuring a strong cooperative environment. These groups have undertaken significant work during the last few years. In particular:

- the Action Group into the law enforcement implications of Electronic Commerce (AGEC) which was convened by the Heads of Commonwealth Operational Law Enforcement Agencies (HOCOLEA).
    - During the last 8 months this group redefined its mandate to ensure continuing viability. This activity saw the creation of several focus groups covering investigations methodology, legal and policy, technical developments and financial sector. The AGEC continued work with the Internet Industry Association (IIA) to finalise a code of practice for Internet Service Providers (ISPs). The code of practice is directed at minimum record keeping standards and appropriate support of investigations conducted by law enforcement and other agencies;
- the E-Security National Agenda, which is a Commonwealth initiative directed at achieving a secure and trusted electronic operating environment. The AFP is a member of the two major inter-departmental working groups created to underpin Commonwealth security arrangements. The two working groups are the E-Security Coordination Group (ESCG) and the Information Infrastructure Protection Group

(IIPG) both of which are chaired by the Commonwealth Attorney General's Department.

- The IIPG is defined as a coordination group chaired by the Attorney General's Department (AGD) that includes the agencies involved in protecting Ausatralia's National Information Infrastructure (NII). The key functional groupings of the NII are telecommunications, banking and finance, transport and distribution, energy and utilities, information services, and other services including defence and emergency. The AFP's role is to respond to any critical NII issues or incidents, respond to and analyse non-critical incidents, identify any related activity which may constitute a critical NII issue and identify strategic issues and trends. The AFP is partnered in this process, through formal joint operating arrangements, with the Australian Security Intelligence Organisation (ASIO) and the Defence Signals Directorate (DSD). The AFP has been granted supplementary funding of $6.8 million over four years from 2002–03 to support its e-security responsibilities.

- The E-Security Coordination Group (ESCG) is chaired by that National Office of the Information Economy (NOIE) and provides a forum for agencies involved in security of Commonwealth bodies that are not necessarily represented through the IIPG. The ESCG charter also encourages it to promote security within the wider economy, which in the past it has pursued through presentations to the Commonwealth IT security community as well as other initiates.

- the Business Government Task Force on Critical Infrastructure Protection. The Task Force was convened by the Prime Minister prior to the Leaders Summit on Counter-Terrorism . This task force made several recommendations to the Prime Minister which were agreed by the National Security Committee of Cabinet (NSC) in a whole of government response in November 2002. Progress on implementation of the recommendations has seen the creation of the Trusted Information Sharing Network (TISN) intended to allow the owners and operators of critical infrastructure to share information on important issues such as business continuity, consequence management, information system attacks and vulnerabilities, e-crime, protection of key sites from attack or sabotage, chemical, biological and radiological threats to water supplies, and the identification and protection of offshore and maritime assets. The TISN is being coordinated through the IIPG (as mentioned in the previous point) and will be overseen by a Critical Infrastructure Advisory Council (CIAC) representing Commonwealth, State and Territory Governments.

- the Australasian Police Commissioners' Conference E-crime Project. This project drives the Electronic Crime Strategy. The AFP was a member of the E-Crime Steering Committee, the E-Crime Working party (ECWP), and an ECWP sub-group. Of particular significance is the fact that the ECWP sub-group drafted an options paper regarding the creation of an Australian High Tech Crime Centre (AHTCC). The project reached a significant milestone in its work, that being the agreement to create an AHTCC. As a result of this decision, it has been agreed by Commissioners that the

E-Crime Project and responsibility for the Electronic Crime Strategy be handed over to the AHTCC.

3. The Australian High Tech Crime Centre (AHTCC)

The concept of an Australian High Tech Crime Centre (AHTCC) was given priority in the work plans of the Police Commissioners' Conference Electronic Crime Strategy of 2001. This identified priority called for an examination of the viability of establishing a genuine cooperative Australian prevention and response capacity.

The major benefit of the AHTCC lies in leveraging the capabilities of each member agency and in the coordination of efforts in fighting high tech crime. The AHTCC will bring national consistency to the management of referrals, training, education, intelligence, target development, policy advice and of course investigations.

The AHTCC will provide significant capacity building opportunities that will improve the sustainability of individual jurisdictions' high tech crime units by providing experience and development of State and Territory members seconded to the AHTCC, as well as through joint operations between the AHTCC and regional units.

Throughout 2001 and into 2002 considerable research into options for a national centre was conducted by members of the ECWP. Following recommendations from Police Commissioners, the formation of the AHTCC was endorsed by the Australasian Police Ministers' Council (APMC) in November 2002.

The role of the AHTCC is to:

- provide a national coordinated approach to combating serious, complex and/or multi-jurisdictional high tech crimes, especially those beyond the capability of single jurisdictions;
- assist in improving the capacity of all jurisdictions to deal with high tech crime; and
- support efforts to protect the National Information Infrastructure.

The AHTCC will achieve this through the following services:

Coordination

✓ providing a single contact point for international agencies, primarily via the AFP international liaison officer network;

✓ maintaining national high tech crime referral arrangements between member agencies; and

✓ providing a contact point for engaging Federal Government agencies.

Investigations

- ✓ providing "triage" services on referrals received and passed to jurisdictions;
- ✓ contributing to investigations conducted by jurisdictions when requested; and
- ✓ conducting investigations into appropriate select matters as defined by the referral arrangements.

Intelligence Services & Products

- ✓ contributing to a better understanding of criminals operating in the high tech crime environment; and
- ✓ providing target identification and target development packages for action by jurisdictions or the AHTCC.

Liaison & Professional Services

- ✓ providing access to forensic advice and assistance;
- ✓ providing access to high tech crime investigations advice and assistance;
- ✓ providing access to specialised technologies and expertise;
- ✓ contributing to ongoing policy development and law reform through centralised advocacy;
- ✓ supporting liaison arrangements between law enforcement and other interested government and non-government organisations; and
- ✓ maintaining a vigorous industry liaison program, particularly in areas of critical national information infrastructure.

Knowledge

- ✓ promoting best practice standards for the prevention, detection and investigation of high tech crime matters;
- ✓ promoting and coordinating training and education; and
- ✓ providing expert advice to jurisdictions on a range of high tech crime issues.

The AHTCC is hosted by the AFP in its National Head Office in Canberra. All Australian police services have agreed to commit staff and resources to the AHTCC. While largely a law enforcement body, other relevant departments and organisations are being engaged to examine the benefit in locating staff within the Centre.

AFP Hosting of the AHTCC

In being hosted by the AFP, the AHTCC will be able to leverage the AFP's existing capacity and relationships in relation to NII and e-security, intelligence, investigations, computer forensics, international liaison, and wider Commonwealth relationships. The AFP is providing a core of up to 19 staff as well as equipment, premises and operating funds.

AHTCC Governance

The strategic direction of the AHTCC is set by the AHTCC Board of Management. The Board is comprised of all Australian Police Commissioners and the Commissioner of the New Zealand Police who has observer status. The current Chair of the Board is Commissioner Mal Hyde of the South Australia Police.

In addition to the Board, a High Tech Crime Managers' Group (HTCMG) has been formed. Senior managers from the various high tech crime investigative units, as well as selected invited institutions such as the Australian Crime Commission (ACC), make up the HTCMG and report to the Board. The HTCMG is a consultative group designed to provide advice and assistance to the Director AHTCC, to ensure national consistency in the activities of operational high tech crime units, and to drive the Electronic Crime Strategy.

AHTCC Operations

The AHTCC will become actively involved in investigations only after having taken due regard for the:

- complexity (multi-jurisdictional or transnational) of the alleged offence;
- degree of specialist technical knowledge and equipment necessary to undertake the investigation;
- capacity of other agencies to carry out the investigation themselves; and
- nature and extent of the criminal impact.

The AHTCC will establish, oversee, and participate where appropriate in effective national and international referral arrangements. However it is neither possible nor desirable for the AHTCC to become the "clearing house" for all high tech crime referrals in Australia as it would risk being inundated by low impact, low priority matters which draw valuable resources away from more significant cases. It is anticipated that most general matters should be addressed by existing jurisdictional investigational mechanisms.

Relationship between the AHTCC and the ACC

The AHTCC is actively engaged with the ACC. The close relationship is illustrated by the above-mentioned membership of the ACC in the HTCMG.

A draft Memorandum of Understanding between the organisations is currently under consideration and will formalise the development and exchange of intelligence relating to high tech crime. That exchange could be further enhanced with the possibility of the ACC attaching an intelligence officer to the AHTCC to work jointly on operations, share intelligence and complement the coordinated efforts of other agencies participating in the AHTCC.

Importantly, it has been recognised that the AHTCC will act as one of the major sources of tactical and strategic intelligence for the ACC on high tech crime matters. The AHTCC in turn sees the ACC as having a significant role in providing a high level understanding of threats and trends. This partnership has already been confirmed through the AHTCC, ACC and a state police service recently conducting a successful joint tactical intelligence operation.

4. LINKS TO THE PJC'S TERMS OF REFERENCE

In relation to the Committee's terms of reference, the AHTCC addresses the following high tech crime types

1. Child Pornography and Associated Paedophile Activity

The Committee has expressed concern about the online availability of images depicting child sexual abuse. The AFP/AHTCC shares this concern and further notes that the availability of such images online represents only one aspect of the broader problems associated with the convergence of child sexual abuse, child pornography and Internet technology. From a societal perspective, each image represents the permanent record of the sexual abuse or exploitation of a child, and the sharing of these abusive images continues the abuse of those children.

Child sex offenders have unfortunately benefited greatly from the technology of the Internet. Their activities online include targeting and "grooming" of future victims, distribution of child pornographic images and facilitation of predatory acts against children themselves.

As with most criminals, the perception of increased anonymity held by most online child sex offenders decreases the perceived risks of detection, which substantially increases their decisions to re-offend. Given that the use of child pornography and associated material is well documented in the development of child sexual abusers, the prevalence and accessibility of this material is of significant concern. Additionally, such material may be used to "normalise" sexual activity between adults/children and children/children, and to gain silence by blackmail.

National Response

The national and international coordination capabilities of the AHTCC are well placed to assist Australian and international police in the investigation of online child sex offenders and with initiatives to further reduce this crime type.

A working group comprised of the Australian Customs Service, Victoria, New South Wales, Queensland and Australian Federal Police (reporting to the Australasian Crime Commissioners Forum) is currently examining the formation of a National Online Child Sexual Abuse Unit (NOCSAU). Subject to deliberations, the Unit could be tasked with implementing an Australasian online strategy for child sexual abuse. Should this decision be taken, the AHTCC Board may be asked to approve the location of the NOCSAU within the AHTCC as a discrete entity.

In terms of legislation, the AHTCC notes that a number of amendments to the *Criminal Code Act 1995* have been proposed by the Commonwealth. These amendments will target the use of the Internet to transmit or download child pornography and are considered a positive first step towards ensuring a national capability to investigate one critical aspect of online child sex abuse.

The AHTCC notes that the Online Child Sexual Abuse Working Group has suggested that offences for online procurement and grooming of children by child sex offenders, as currently exist in a few Australian jurisdictions, would further add to the tools and mechanisms available to Australian law enforcement agencies. The uniform inclusion of such offences in State, Territory and Commonwealth legislation could provide a useful preventative mechanism for law enforcement intervention prior to the actual physical act of child sexual abuse occurring.

2. Banking, including Credit Card Fraud and Money Laundering

Significant investigations have recently been conducted by the AFP into frauds carried out against customers of Australian Internet banking services, most notably involving arrests in both New South Wales and South Australia. These investigations have operated in conjunction with state law enforcement and AFP liaison within the banking industry.

Different methods have been used to carry out these frauds, however all rely on traditional fraud methods in which customers are deceived into providing personal information which has been used to facilitate unauthorised funds transfer via online banking systems. It is important to note that none of these incidents have involved compromise to bank systems themselves.

In addition to State and Territory dishonesty and money laundering offences, the Commonwealth's *Cybercrime Act 2001* provisions in the *Criminal Code Act 1995* (Section 478.1-Unauthorised access to, or modification of, restricted data) as well as the money laundering provisions in the *Criminal Code Act 1995* (Section 400.7 relating to the handling of proceeds of crime) provide valuable avenues for investigation.

The national and international capabilities of the AFP, in particular through cooperation with state law enforcement and the banking industry (through membership of groups such as the Australian Bankers Association Fraud Taskforce and relationships with overseas law enforcement agencies) has proven to be vital in achieving results in these international and multi-jurisdictional crimes.

This multi-faceted approach, which will form the basis of AHTCC operations, will ensure not only successful investigations, but will allow the AHTCC to identify other avenues for addressing high tech crimes.

Credit card skimming has also been a topic of recent media scrutiny. The AHTCC's role in relation to credit card skimming will be no different to any other type of illegal activity in that investigative action would be dependant on those factors detailed in the *AFP Operations* section earlier in this paper, specifically the complexity of the offending and the degree of specialist technical knowledge and equipment necessary to undertake the investigation.

3. Threats to National Critical Infrastructure

The National Information Infrastructure (NII) fits within the broader concept of Critical Infrastructure, and is formed by the interconnected networks of essential services such as telecommunications, banking and finance, transport and distribution, energy and utilities, information services, and other services including defence and emergency. Potential threats to the NII include acts by individuals, terrorist groups, or even foreign governments.

The AFP was granted supplementary funding of $6.8 million over four years from FY02 to support its e-security responsibilities. Given the core role of the AFP within the AHTCC, the AHTCC will be the main Australian law enforcement unit involved in the investigation of an electronic threat or electronic attack against the NII.

Under the auspices of the AFP, the AHTCC will be party to a formal Joint Operating Arrangement (JOA) with the Australian Security Intelligence Organisation (ASIO) and the Computer Network Vulnerability Team of the Defence Signals Directorate (DSD). The JOA provides guidance on the role of each agency in the instance of an electronic threat against the NII. The JOA partners meet on a regular basis and are actively working towards strengthening reaction capacity in the event of a threat.

The AHTCC will take the lead in criminal matters involving the NII, but it is widely recognised that state and territory police services may be the first responders in any attack against the NII. As with other matters in which the AHTCC will be involved, the established cooperative agreements with the various high tech crime units will put the AHTCC and the relevant local services in a good position for effective response. The sharing of skills and resources, as well as information and intelligence in the field of NII investigation is critical, and the AHTCC will provide a useful vehicle for that purpose.

As previously mentioned in the section *Australian High Tech Crime Centre*, the AHTCC's access to overseas partner agencies at an operational level (facilitated by the AFP International Liaison Officer Network) will ensure that the AHTCC is well positioned to react to and investigate electronic threats and attacks against the NII.

In addition to the above investigative relationships with Commonwealth, State and Territory agencies, the AHTCC will be an active participant in a range of fora designed to increase responsiveness, cooperation and effectiveness in the field of NII protection. These include:

- The Australian 24-hour emergency contact point for the G8 Subgroup on high-tech crime. The contact point network now encompasses 23 countries.

- The AFP operates a considerable international network comprising of 65 officers and advisors located across 32 posts in 26 countries worldwide.

- The AFP acts as the National Central Bureau for Interpol, and consequently the Interpol Central Reference Point for computer-related crime.

- The AHTCC will participate in the Action Group into the law enforcement implications of Electronic Commerce (AGEC), convened by HOCOLEA.

- The AFP is a major participant in the E-Security National Agenda, which is a Commonwealth initiative directed at achieving a secure and trusted electronic operating environment. The AFP is a member of the two major inter-departmental working groups created to underpin Commonwealth security arrangements, these being the E-Security Coordination Group (WSCG), E-Security Working Group (ESWG) and the Critical Infrastructure Protection Group (CIPG) in conjunction with the Commonwealth Attorney General's Department (AGD) and the National Office of the Information Economy (NOIE). The critical involvement will continue with the AHTCC.

- The AHTCC will participate in the Trusted Information Sharing Network sponsored by AGD and recommended by the Business Government Task Force on Critical Infrastructure Protection.

- The AHTCC/AFP, in conjunction with the Commonwealth AGD and other Commonwealth agencies, will subscribe to the National Incident Reporting Scheme run by AusCERT, which will act as a "front door" for IT security incident reporting from the private sector.

- The AFP has recently negotiated a training contract with AusCERT for the provision of expert training on the investigation of network attacks. This training will be leveraged by the AHTCC.

- The AFP/AHTCC partnered with AusCERT, Queensland Police, Western Australia Police and South Australia Police in the *2003 Australian Computer Crime and Security Survey.* The Survey provides a unique and valuable insight into the level, nature and complexity of, as well as the damage caused by, IT security incidents against Australian business.

- The AFP/AHTCC participated in a multi-agency working group convened by Standards Australia to produce Guidelines for the Handling of IT Evidence. Production of this guideline was sponsored by the AFP and the Commonwealth AGD.

Finally, the *Cybercrime Act 2001* provisions in the *Criminal Code Act 1995* provide a useful legislative base for criminal investigations involving attacks on the NII, including offences such as unlawful access to data, alteration of data, impairment of electronic communications, and creation and distribution of malicious software. These provisions have ensured that activities which are considered unlawful by modern day standards can be effectively investigated by the AFP/AHTCC. Other provisions in relation to search and seizure are adequate for modern high tech crime investigations.

Research Priorities

The AHTCC notes that the Commonwealth through the Department of Education, Science and Training has recently set *Safeguarding Australia* as one of four National Research Priorities. The research goals of this priority are:

1. Critical infrastructure;
2. Protecting Australia from invasive diseases and pests;
3. Protecting Australia from terrorism and crime; and
4. Transformational defence technologies.

The AHTCC will share an interest in the goals of critical infrastructure and protecting Australia from terrorism and crime, and as such believes these research priorities provide opportunities for partnering with research agencies in order to better address these issues of national concern.

5. Conclusion

The environment in which law enforcement and regulatory agencies must operate is increasingly complex. While advances in technology have provided new opportunities for commerce, employment and communication, they have equally facilitated criminal activity.

The formation of the Australasian High Tech Crime Centre illustrates the mature approach with which Australia's law enforcement agencies intend to address these issues through cooperation in developing capability, acquiring appropriate tools, pursuing law reform, and ensuring robust international relationships.