Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:25
Received 1 July 2003

Mr Bill Kelly
Deputy Commissioner (Operations
Victoria Police
PO Box 415
MELBOURNE VIC 3005
☎03 9865 2754 🖹03 9865 2769
E-mail:

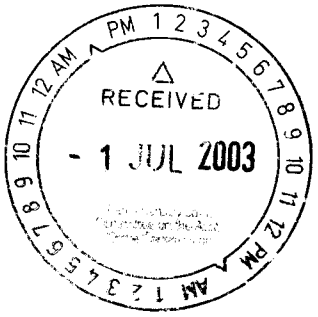
VICTORIA POLICE

Office of the Deputy Commissioner, Operations

Victoria Police Centre
637 Flinders Street
Melbourne Victoria
Australia 3005
Telephone [61 3] 9247 6803
Facsimile [61 3] 9247 6818

P.O. Box 415
Melbourne Victoria
Australia 3005

Ms. Maureen Weeks
Committee Secretary
Parliamentary Joint Committee on the Australian Crime Commission
Parliamentary House
Canberra ACT 2600



Victoria Police Submission to the Parliamentary Joint Committee on the Australian Crime Commission

Dear Ms. Weeks

In response to the request from the Parliamentary Joint Committee, the Assistant Commissioner (Crime), Simon Overland has coordinated preparation and authorised release of materials relevant to the scope of the request. It is noted that the inquiry will examine *recent* trends in cybercrime techniques and practices with particular reference to:

- Child pornography and associated paedophile activity;
- Banking, including credit card fraud and money laundering; and
- Threats to national critical infrastructure.

The following points were identified as relevant to each of the above sub issues:

Child pornography and associated paedophile activity

- Global nature of Internet environment making communication between paedophiles easier;
- Ability for paedophile groups to meet in on-line chat rooms and exchange images;
- Greater knowledge of technology and the use of encryption and steganography;
- Anonymity and the danger of young children being targeted by paedophiles adopting an on-line profile of a young child; and

- Recent Interpol initiative (child pornography database development) and the provision of assistance to international law enforcement.

Banking, including credit card fraud and money laundering

- Magnetic card cloning;
- Credit card skimming;
- Website duplication to obtain customer credit card and on-line banking details;
- Fraudulent documentation generation to obtain loans; and
- Identity theft (please refer attachment 'C').

Threats to national critical infrastructure

- Recent experience of investigative assistance provided by the Computer Crime Squad regarding threats made via email against Melbourne Water to remotely detonate drums of cyanide allegedly planted in water reservoirs;
- Issues surrounding greater use of email to commit stalking or to deliver threats; and
- Issues for law enforcement agencies regarding interception of email messages.

As previously indicated by you on behalf of the PJC, the statistical material generated by the Victoria Police Computer Crime Squad in terms of annual workloads, offence types investigated and associated increase trends should be particularly relevant and of interest to deliberations of the committee. Materials related to those aspects form attachment 'A'.

Further attachments constitute materials that may be of interest to the committee, namely:

- Attachment 'B': Victoria Police Proclamation Law Memo (May 2003), providing a summation of the of the recent passed *Crimes (Property Damage and Computer Offences) Act* 2003;
- Attachment 'C': Policy document titled *Australian Identity Crime Policing Strategy*
- Attachment 'D': Interpol Media Release titled *Major Child Pornography Operation Broken in Sweden.*

I trust that the materials will be of value to the committee's deliberations. The coordination / contact person in relation to this issue is Inspector Brad Shallies, Legal & Corporate Policy, on (03) 9247 6729.

Bill Kelly
Deputy Commissioner (Operations)

26/6/03.

APPENDIX A

VICTORIA POLICE - COMPUTER CRIME SQUAD
WORK ANALYSIS HISTORY AND PROJECTIONS

This document contains an analysis of the historical, current and projected workloads of the Victoria Police Computer Crime Squad (CCS). It is intended to provide the reader with a factual, historical overview of the functions and tasks undertaken by the squad, the past and present effects of rapidly changing technology and its uptake in the community on both the frequency and complexity of those tasks, and an analysis of those effects on the ability of the squad to continue to service its core functions and meet the expectations of the community and Victoria Police.

Throughout the report there will be references to the volume of data analyzed expressed in Gigabytes (Gigs). To provide an understanding in layman's terms of the quantity of data stored in a gigabyte, a floppy disk will hold 1.44 Megabytes. This is equivalent to a text document containing approximately 1,400,000 characters or 230,000 words. In broad terms, one Gigabyte (1,000,000,000 bytes) = 1000 Megabytes or approximately 230,000,000 words. To put this in perspective, all the words, pictures, sound files and movie clips contained in the 2000 Encyclopedia Britannica, fit on one 650 megabyte CD-ROM, Wright State University U.S.A., in a news release dated 16/6/2000, contends that 3.5 Gigabytes of data equates to a stack of documents the height of the Eiffel Tower.[1]

The statistical data in this review was drawn from the internal job database of the CCS, which has been in use since 1997. Data for the fiscal year 1993-1994 to the commencement of the database was back captured shortly after it came into service. The annual figures for the 2002-2003 fiscal year were projected by extending the data captured during the first 8 months of that fiscal period. Projected figures (shown in blue text) for the fiscal years 2003-2004 to 2007-2008 were calculated using the Microsoft 'Trend Growth Analysis' function based on the previous 4 years of data.

Table 1.1 represents the total number of tasks undertaken by the CCS on an annual basis, the annual percentage increase of tasks attended to, and the expected projected workloads for the following 5 years along with the variance increase of tasks since the fiscal year 1994-1995.

Total number of tasks annually					
Fiscal Year July to June	**Analysis Tasks**	**Other Tasks Attended**	**Total No. Attended**	**% Job Count Increase P/A**	**% Variance Since 1994/5**
1993 - 1994	51		51		
1994 - 1995	73		73	43.13	0
1995 - 1996	98		98	34.24	34.24
1996 - 1997	161		161	64.28	120.54
1997 - 1998	104	135	239	48.44	227.39
1998 - 1999	144	404	548	129.28	650.68
1999 - 2000	180	299	479	-12.6	556.16
2000 - 2001	222	366	588	22.75	705.47
2001 - 2002	343	336	679	15.47	830.13
2002 - 2003	436	443	879	29.45	1104.10
2003 - 2004	601	469	1070	21.72	1365.75
2004 - 2005	819	523	1342	25.42	1738.35
2005 - 2006	1116	584	1700	26.67	2228.76
2006 - 2007	1520	652	2172	27.76	2875.34
2007 - 2008	2070	727	2797	28.77	3731.50

Table 1.1

APPENDIX A

Chart 1.1 depicts the total tasks attended by the CCS as represented in table 1.1 and graphically represents the increasing workload trend and projections.

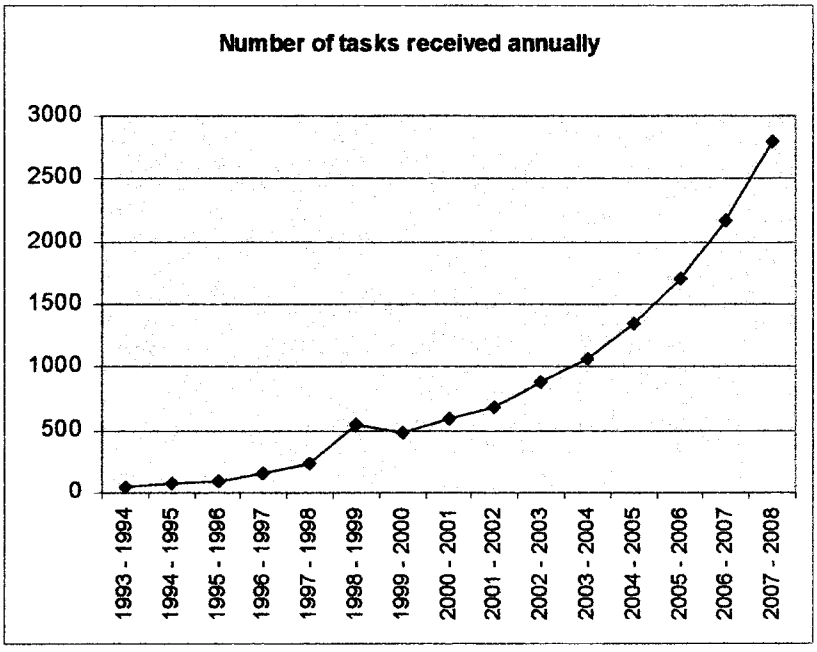


Chart 1.1

The core functions of the CCS include the conduct of investigations requiring complex technical knowledge or skills, forensic computer analysis (including analysis of other technologies), Industry and ISP liaison, and investigative assistance including scene search and seizure, case assessments, assisting informants with suspect or witness interviews, SIM card analysis and other assistance. A breakdown of the annual tasks for the 6 year period 1997 to 2003 is provided in table 2.1. The 'Analysis Tasks' total represents the combined number of Evidence Analysis and Search and Seizure tasks undertaken.

Breakdown of annual tasks						
Task Category	**1997-1998**	**1998-1999**	**1999-2000**	**2000-2001**	**2001-2002**	**2002-2003**
Evidence Analysis	72	110	150	182	261	340
Search & Seizure	32	34	30	40	82	96
Investigation Assist	60	308	266	279	235	294
CCS Invest	49	67	12	1	1	1
Sus / Wit Interview	7	15	1	0	0	0
Case Assessment	15	10	5	1	1	1
SIM Card Analysis	0	2	13	75	91	119
Other Task	4	2	2	10	8	28
Totals	**239**	**548**	**479**	**588**	**679**	**879**
Analysis Tasks	**104**	**144**	**180**	**222**	**343**	**436**

Table 2.1

APPENDIX A

As evidenced by the figures, in table 1.1 and table 2.1 there has been a consistent and steadily increasing workload placed on the CCS since 1993. However, in the 1998-1999 fiscal year, the number of requests for investigative assistance soared due to the sudden increase in the number of frauds being committed on Internet Service Providers (ISPs) and/or their clients. Not at all surprising when one considers that according to the Australian Bureau of Statistics, as at May 1998, more than 970,000 Australian homes had home internet access, an increase of over 14% on the previous year[2]. (In the 2001 census almost 8 Million Australians had access to the internet from home[3].) At that time the CCS had also adopted the role of ISP liaison point for Victoria Police. On identifying this issue, the CCS immediately instituted a national push to hold ISPs responsible for their lax on-line signup procedures and client account security. As a result, after several meetings with the top three Internet Service Providers and the Internet Industry Association (IAA), the CCS developed an ISP fraud reporting methodology which in essence has held ISPs to account, and made it incumbent upon them to provide an evidence package with each report made. Consequently, the previously rising tide of reported ISP related frauds, and therefore the associated request for investigative assistance, was stemmed and the number of reported frauds dropped.

The Internet, however, has continued to gather momentum as the new means to commit old offences and has remained a consistent influence on the 'investigate assistance' sought from the CCS. On the other hand requests for forensic computer analysis, including the scene analysis associated with warrant search and seizure, has continued to grow at an ever increasing pace, as is evidence in chart 2.1.

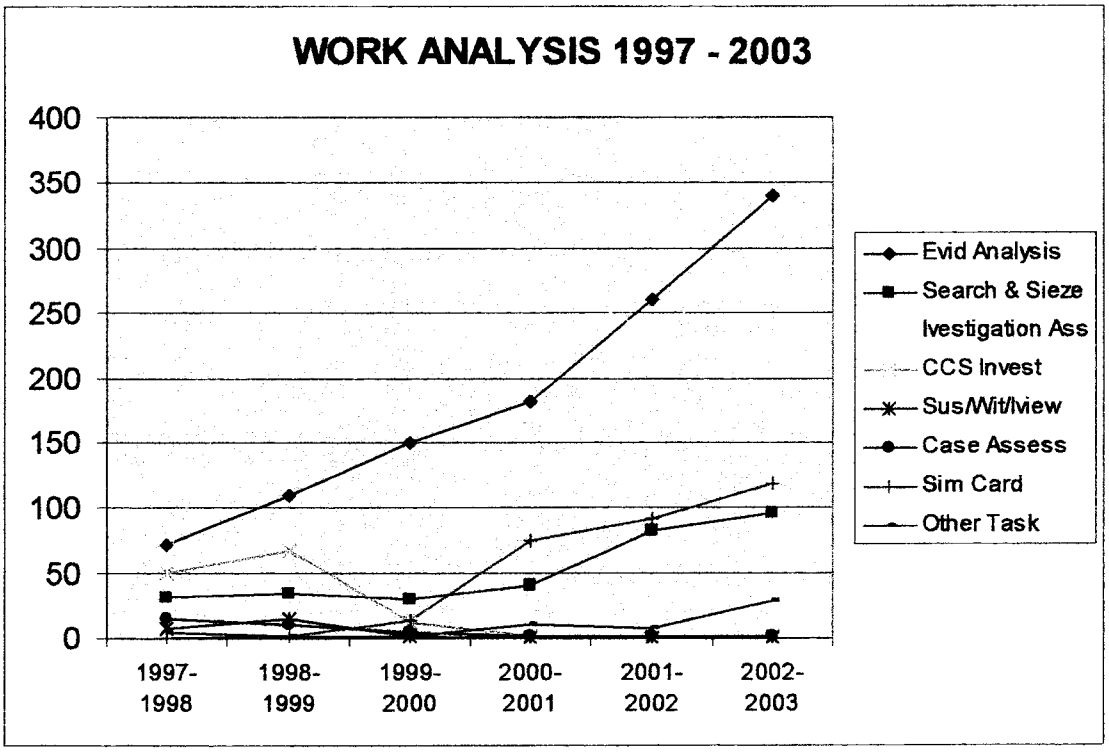


Chart 2.1

APPENDIX A

Table 3.1 and charts 3.1 & 3.2 provide a detailed analysis of the computer analysis tasks being undertaken by the squad and highlight the resulting impact of ongoing development in HDD technology.

Number of computer analysis tasks					
Fiscal Year July to June	No. of Analysis Tasks	Avg. Data Analysed In Gigabytes	Total Data Analysed in Gigabytes	Annual % Variance	Analysis % Increase Since 97/98
1993 - 1994	N/A				
1994 - 1995	N/A				
1995 - 1996	N/A				
1996 - 1997	N/A				
1997 - 1998	104	1.50	156		0
1998 - 1999	144	2.28	329	110.89	110.89
1999 - 2000	180	5.94	1069	224.92	585.25
2000 - 2001	222	9.41	2089	95.41	1239.10
2001 - 2002	343	13.28	4555	118.04	2819.87
2002 - 2003	436	14.99	6537	43.51	4090.38
2003 - 2004	601	22.45	13493	106.40	8549.35
2004 - 2005	819	30.66	25113	86.11	15998.07
2005 - 2006	1116	41.88	46739	86.11	29860.89
2006 - 2007	1520	57.23	86988	86.11	55661.53
2007 - 2008	2070	78.21	161895	86.11	103678.84

Table 3.1

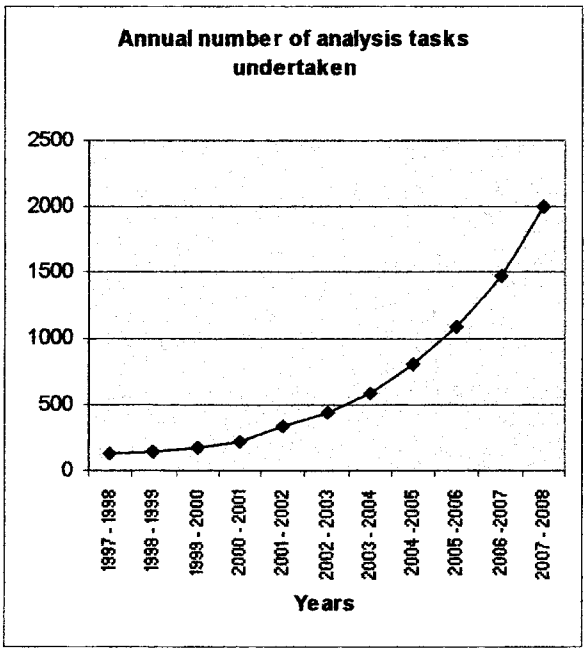


Chart 3.1

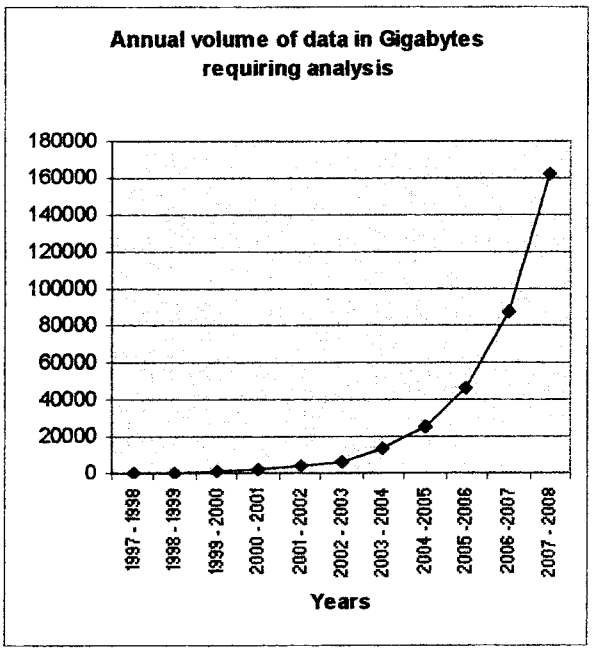


Chart 3.2

It is not difficult to conclude that the technological advances in storage medium must have a finite limit and eventually will level off. Unfortunately, this is just not so according to Dave Reinsel, the Research

Manager of Hard Disk Drives of IDC, a leading US research company[4] who has provided the following research on HDDs.

Desktop HDD sizes available per annum in Gigabytes														
1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003e	2004e	2005e	2006e
0.8	1.2	2.4	4.3	6.4	12	20	40	80	160	320	320	500	750	1000

Table 4.1

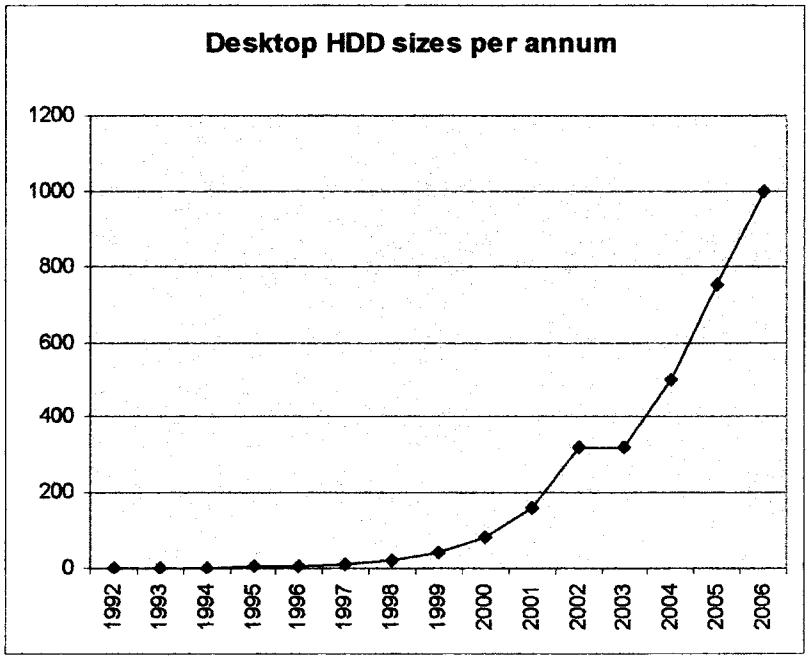


Chart 4.1

Reinsel is not alone in his predictions. In a research paper prepared for the Computing Science section of the May-June 2002 edition of the American Science journal[5], Brian Hayes, a senior writer for the journal, mirrored Reinsel predictions, and further estimated that HDD capacity would reach a 120 Terabytes by the year 2012. I Terabyte = 1000 Gigabytes. Hayes also made comment on the tumbling cost of the technology placing hard drives of such capacity well within the reach and budget of ordinary home PC users.

In the event that their research is correct, and that HDD capacity continues to grow as predicted, then the projections outlined in this paper may well be grossly understated, for the entire data volume analysed by the squad this year would be housed in only 6 HDDS by the year 2005-2006 or 4 by 2006-2007, somewhat significantly less than the predicted 1116 projected requests for analysis for 2005-2006. This would be aside from any analysis required on palm tops, hand held PC, mobile phones and the myriad of other advancing data devices which are even now propagating the technological market place.

Data volumes of this magnitude, of itself rings alarm bells, and raises a great many issues relating to the methodologies required to analyse and back-up the evidentiary data located. Significant research and tool development will need to be undertaken to deal with these emerging problems; however those issues are outside the scope of this paper and will not be further addressed herein.

The rapid growth and projected data volumes come as no surprise to the members of the squad. Table 5.1 and Chart 5.1 depict the historical, current and projected analysis workload of the individual Squad

personnel. Staffing levels have been adjusted to account for annual leave, and future projections are based on the current staffing levels of the squad.

Data volume analysed per staff member annually					
Fiscal Year July to June	Data volume in Gigabytes	# Members (Leave Adjusted)	Volume Per Member in Gigabytes	% Increase P/A	% Increase since 97- 98
1997 - 1998	156	5	31		
1998 - 1999	329	7	47	51.61	51.61
1999 - 2000	1069	7	152	223.40	390.32
2000 - 2001	2089	8	261	71.71	741.93
2001 - 2002	4555	8.5	535	104.98	1625.80
2002 - 2003	6537	9	726	35.70	2241.93
2003 - 2004	13493	9	1499	106.47	4735.48
2004 -2005	25113	9	2790	86.12	8900.00
2005 -2006	46739	9	5193	86.12	16651.61
2006 -2007	86988	9	9665	86.11	31077.41
2007 - 2008	161895	9	17988	86.11	57925.80

Table 5.1

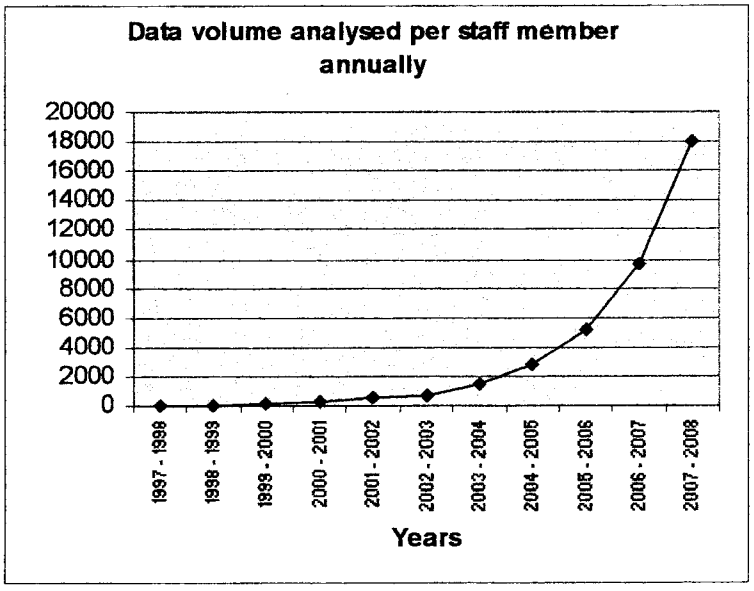


Chart 5.1

HDD growth alone sets a daunting task and yet this is only one aspect of the spiraling demands that technology will place on the Force as a whole. Previously mentioned in this paper was the proliferation of mobile phones, hand held computers and other storage devices that are now becoming part of every day life in society, including the criminal society. In the past few years the Squad has seen the increasing use of encrypted communications between drug traffickers and child pornographers. Emails and SMS messages are now the norm instead of reserved to those select few who could afford the latest advanced technology. The Internet has opened the flood gates to a whole new dimension of offences including stalking, identity theft, on-line fraud, hacking and criminal damages by virus or Trojan. The new Crimes (Property Damage and Computer Offences) Act 2003 is about to be passed in Parliament and will add a myriad of offences to those currently impacting on the workload of the Squad; i.e. Sabotage or Threats of sabotage (aimed at the

protection of the State's infrastructure and commerce), Unauthorized assess or modifications to restricted data, Unauthorised impairment of data held in a computer disk, credit card or other device and Unauthorised impairment of electronic communications are just a few.

The impact of technology is far reaching, but even in the short term it is reasonable to expect that the time necessary to conduct a computer analysis will continue to grow due to the greatly increased data volumes. Training to overcome this will become a major issue as more and more advanced technologies and tools are developed. Tools and equipment will need to remain as cutting edge as those in the hands of the offenders perused. General police members will need to be trained in-line with the 'Computer Investigation' training competencies recently endorsed by the Commissioners' forum.

The advancement of technology has been the burden and yet also brought some blessings. With the aid of more sophisticated software, increased processing power, greater network communication and shared information between forensic practitioners globally and with the personal skill development of the current personnel, the Squad has been able to absorb much of the impact and rise to the challenge of increased workloads measured in the hundreds of percent in just a few short years. However the tide of technology is accelerating beyond the Squad's ability to respond. It has permeated every aspect of society and may in some way be involved in virtually every offence imaginable; for communication, a repository for evidence, a target of, or the tool with which to commit the offence. It is interesting to note that in the fiscal year 2001-2002 the third most prevalent offence in which the CCS assisted was homicide, closely followed by drug related matters and then sexually related offences (other than child pornography which was the second most prevalent offence). Others include Stalking, Armed Robbery, Kidnapping and Blackmail.

Even with the dedication and the best endeavors of the current staff, the workload has and will continue to grow exponentially.

APPENDIX A

Reference Document - Bibliography

1. **Wright State University News Release dated 16th of June 2000.**
   URL: www.wright.edu/cgibin/news_item.cgi?50

2. **Australian Bureau of Statistics, media release 8147.) 'Home internet use grows strongly' dated 25/8/1998. www.abs.gov.au**

3. **Australian Bureau of Statistics 2001 Census of Population and housing. B16 – Internet use by sex.**

4. **Email received from Dave Reinsel, the Research Manager of Hard Disk Drives, of IDC.**

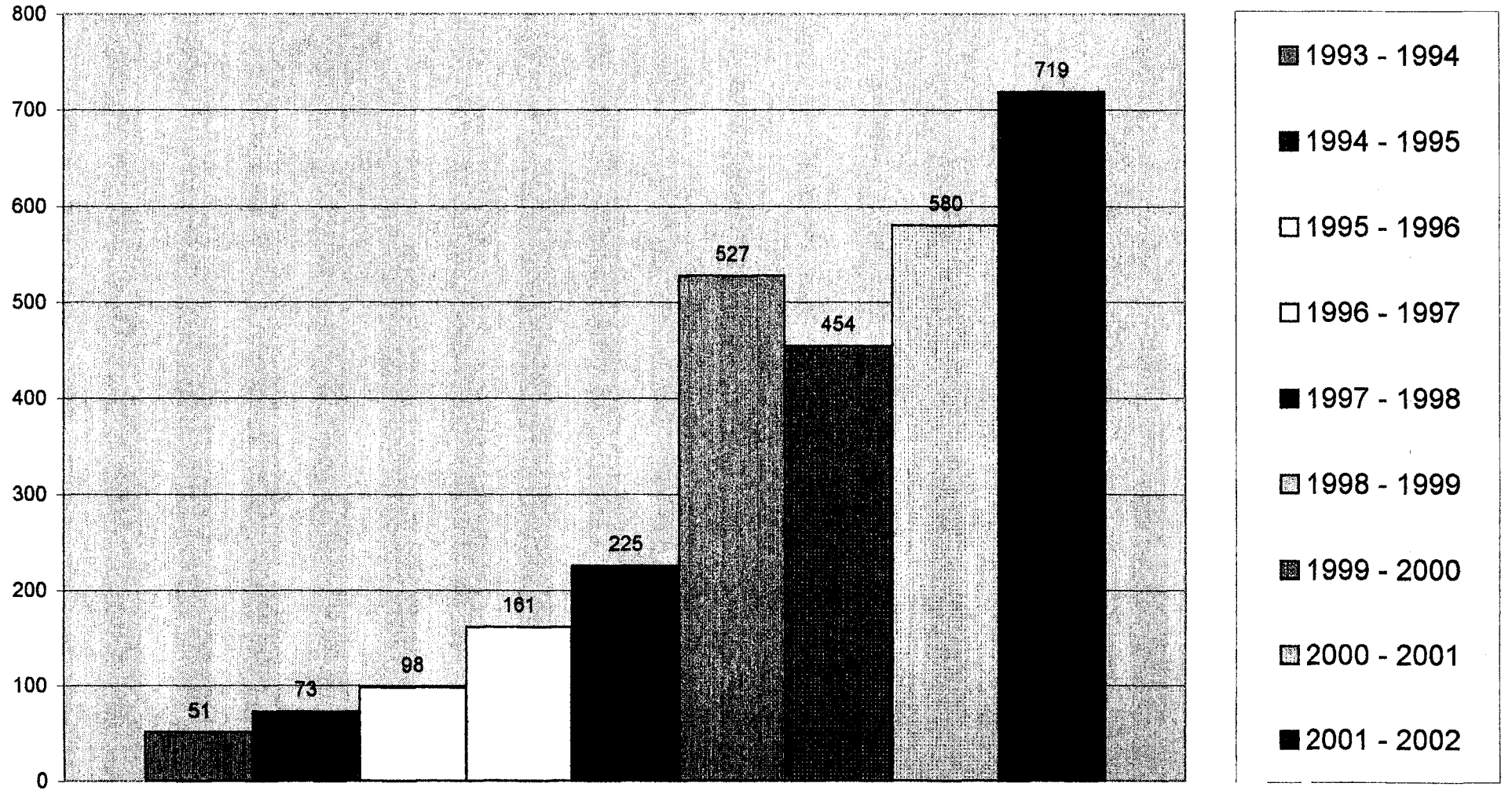
5. **American Scientist Volume 90, dated May-June 2002. Article on page 212 entitled 'Terabyte Territory'**

Computer Crime Investigation Squad

Fiscal Year Workloads 1994 - 2002

(Includes Analysis & ISP Statistics)

VICTORIA POLICE



Peter WHEELER
Detective Senior Sergeant 22088
Officer in Charge - Computer Crime Investigation Squad

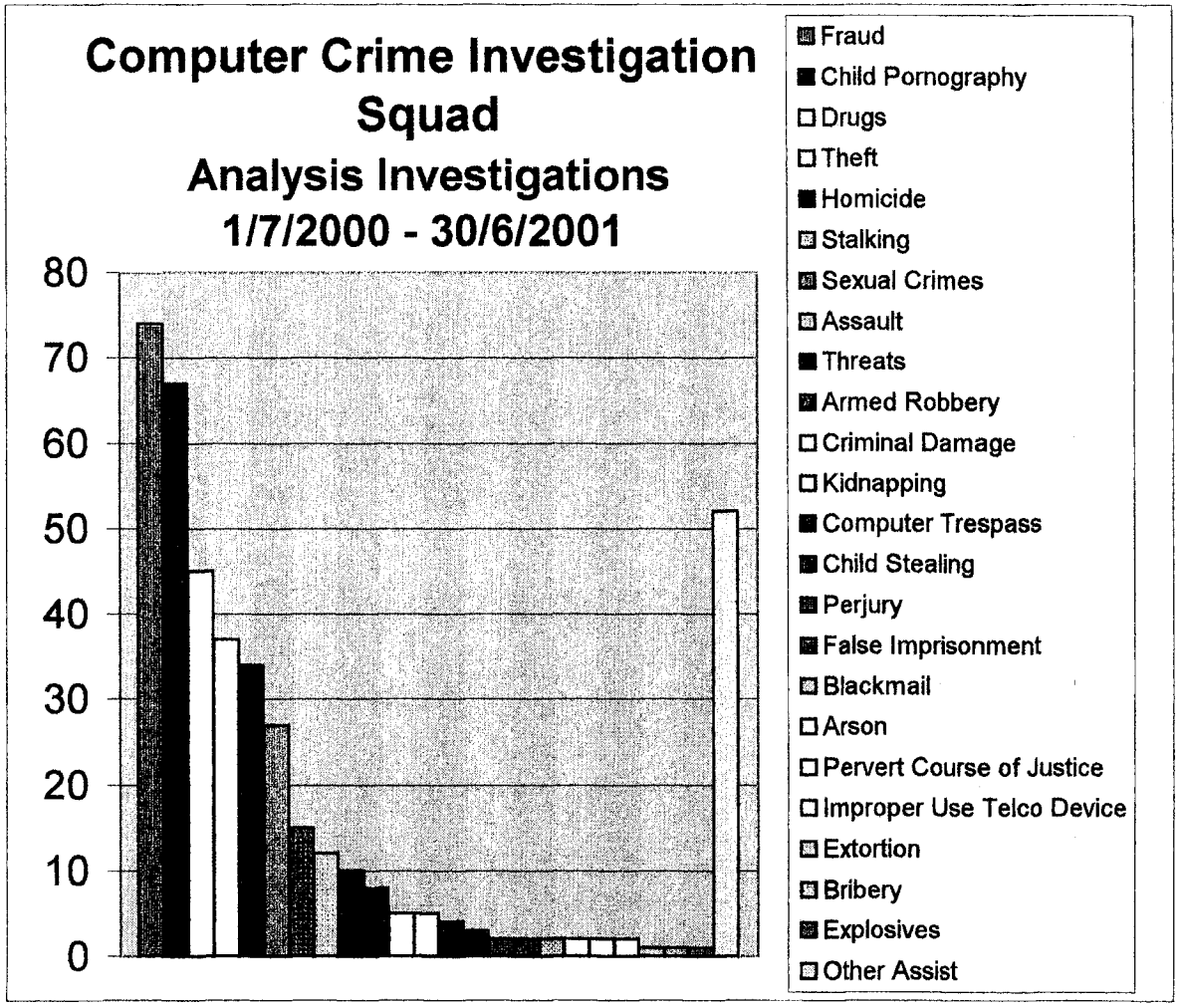
VICTORIA POLICE

Computer Crime Investigation Squad

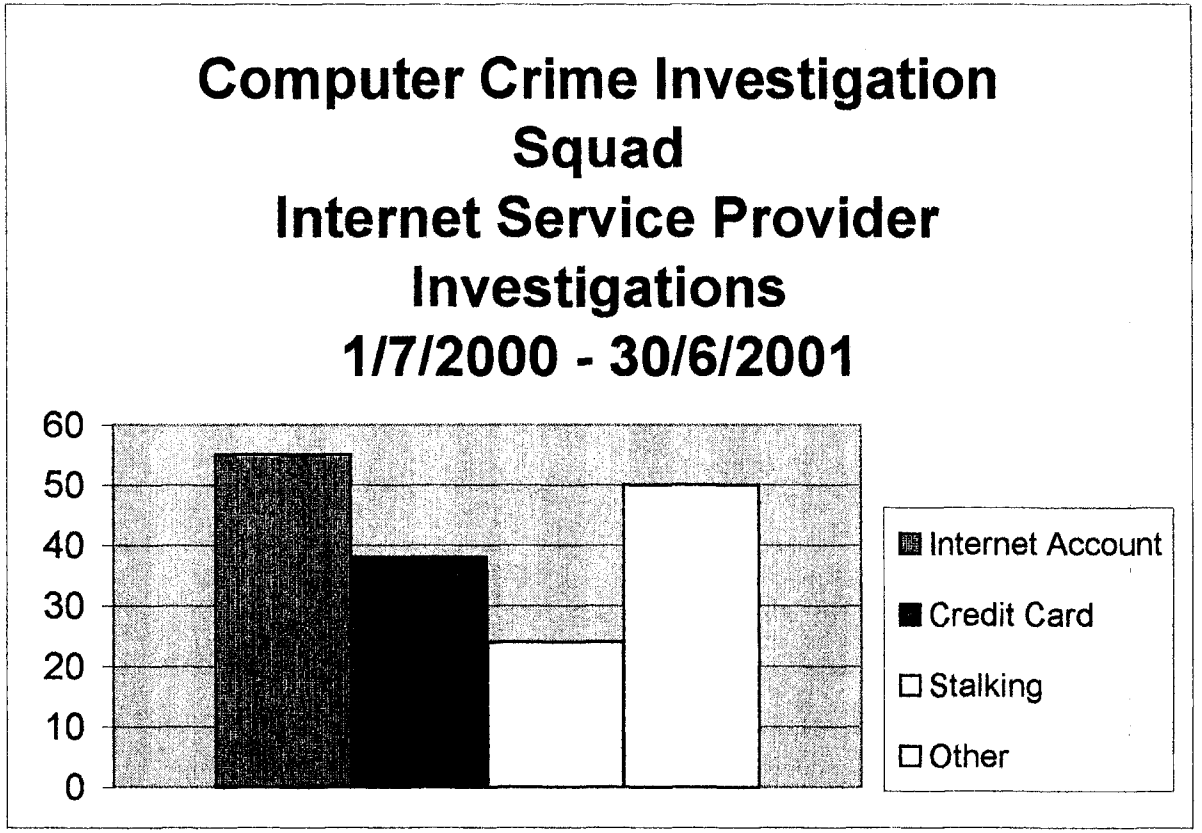
Annual Workloads 1994 - 2002 Statistics

Total No. of Analysis / Investigation & ISP Jobs Statistics						Analysis Jobs Only Statistics				
Fiscal Year	No. of Jobs	ISP Assist Tasks	Total No. of Jobs Attended	Annual % of Job Count Variance P/A	% Job Variance Since 1994/5	No. of Analysis Jobs	Avg. HDD Space Analysed	Total Analysed in Gigabytes	Annual % Analysis Completed Variance	Analysis % Increase Since 97/98
1993 - 1994	51		51			N/A				
1994 - 1995	73		73	43.14	0.00	N/A				
1995 - 1996	98		98	34.25	34.25	N/A				
1996 - 1997	161		161	64.29	120.55	N/A				
1997 - 1998	225		225	39.75	208.22	99	1.2 Gig	118.8	N/A	0
1998 - 1999	378	149	527	134.22	621.92	111	4 Gig	444	273.74	273.74
1999 - 2000	226	228	454	-13.85	521.92	164	7.6 Gig	1246.4	180.72	949.16
2000 - 2001	413	167	580	27.75	694.52	181	9.3 Gig	1,679.40	34.74	1313.64
2001 - 2002	539	180	719	23.97	884.93	270	11.6 Gig	3,131.20	86.45	2535.69

Fraud	74	17.92%
Child Pornography	67	16.22%
Drugs	45	10.90%
Theft	37	8.96%
Homicide	34	8.23%
Stalking	27	6.54%
Sexual Crimes	15	3.63%
Assault	12	2.91%
Threats	10	2.42%
Armed Robbery	8	1.94%
Criminal Damage	5	1.21%
Kidnapping	5	1.21%
Computer Trespass	4	0.97%
Child Stealing	3	0.73%
Perjury	2	0.48%
False Imprisonment	2	0.48%
Blackmail	2	0.48%
Arson	2	0.48%
Pervert Course of Justice	2	0.48%
Improper Use Telco Device	2	0.48%
Extortion	1	0.24%
Bribery	1	0.24%
Explosives	1	0.24%
Other Assist	52	12.59%
	413	100.00%



Internet Account	55	33%
Credit Card	38	23%
Stalking	24	14%
Other	50	30%
	167	100%

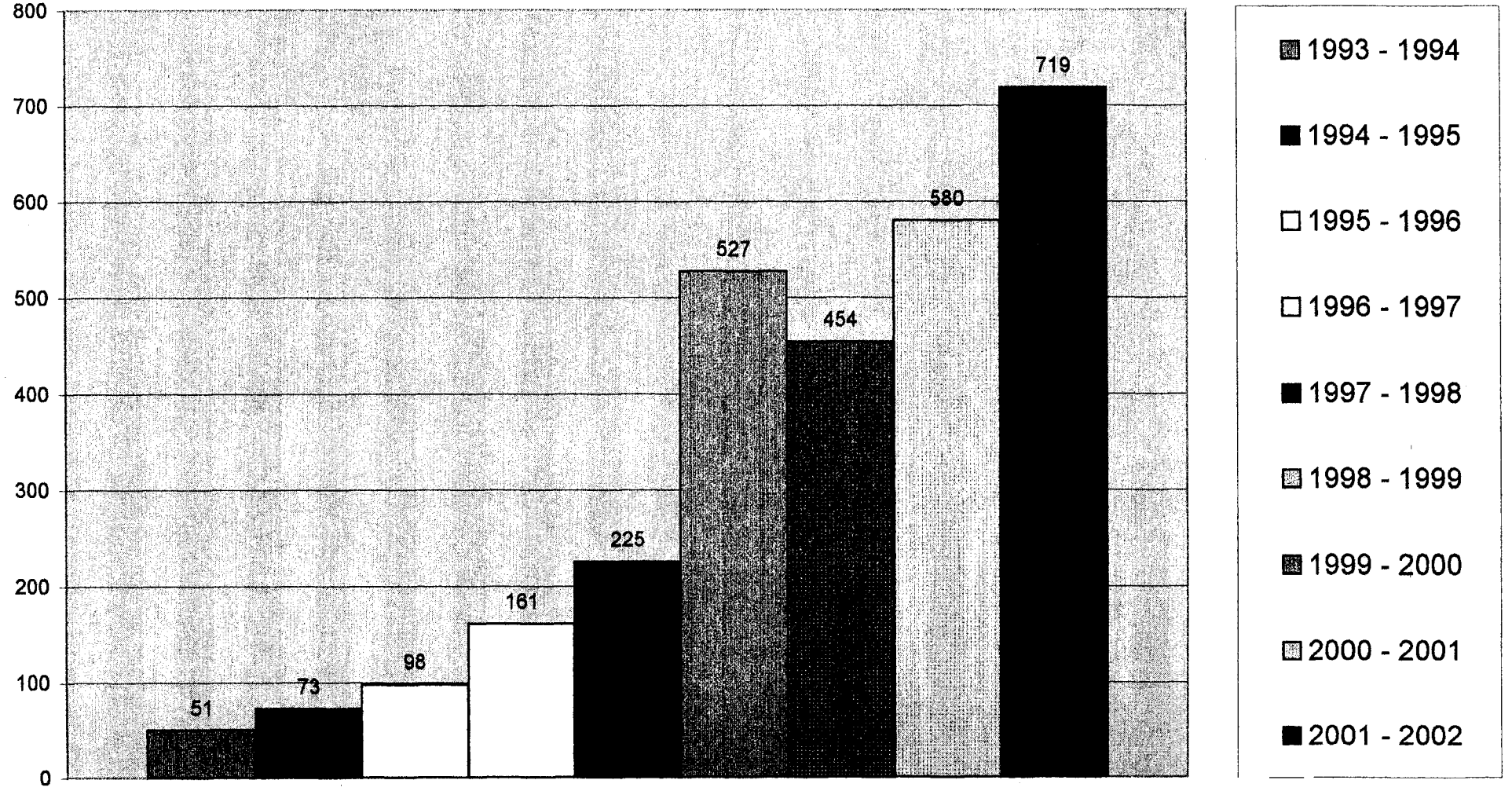


VICTORIA POLICE

Computer Crime Investigation Squad

Fiscal Year Workloads 1994 - 2002

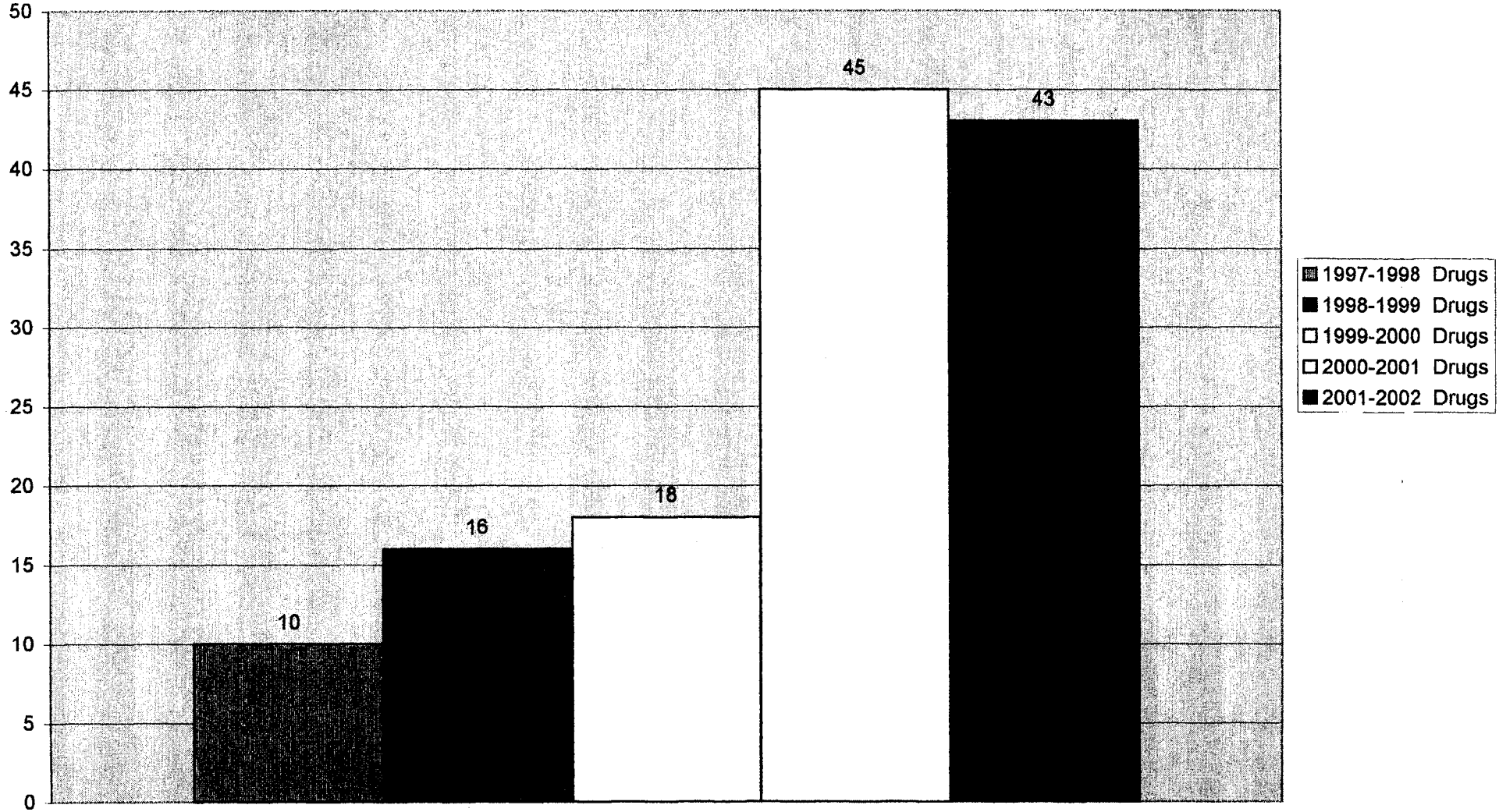
(Includes Analysis & ISP Statistics)



Peter WHEELER
Detective Senior Sergeant 22088
Officer in Charge - Computer Crime Investigation Squad

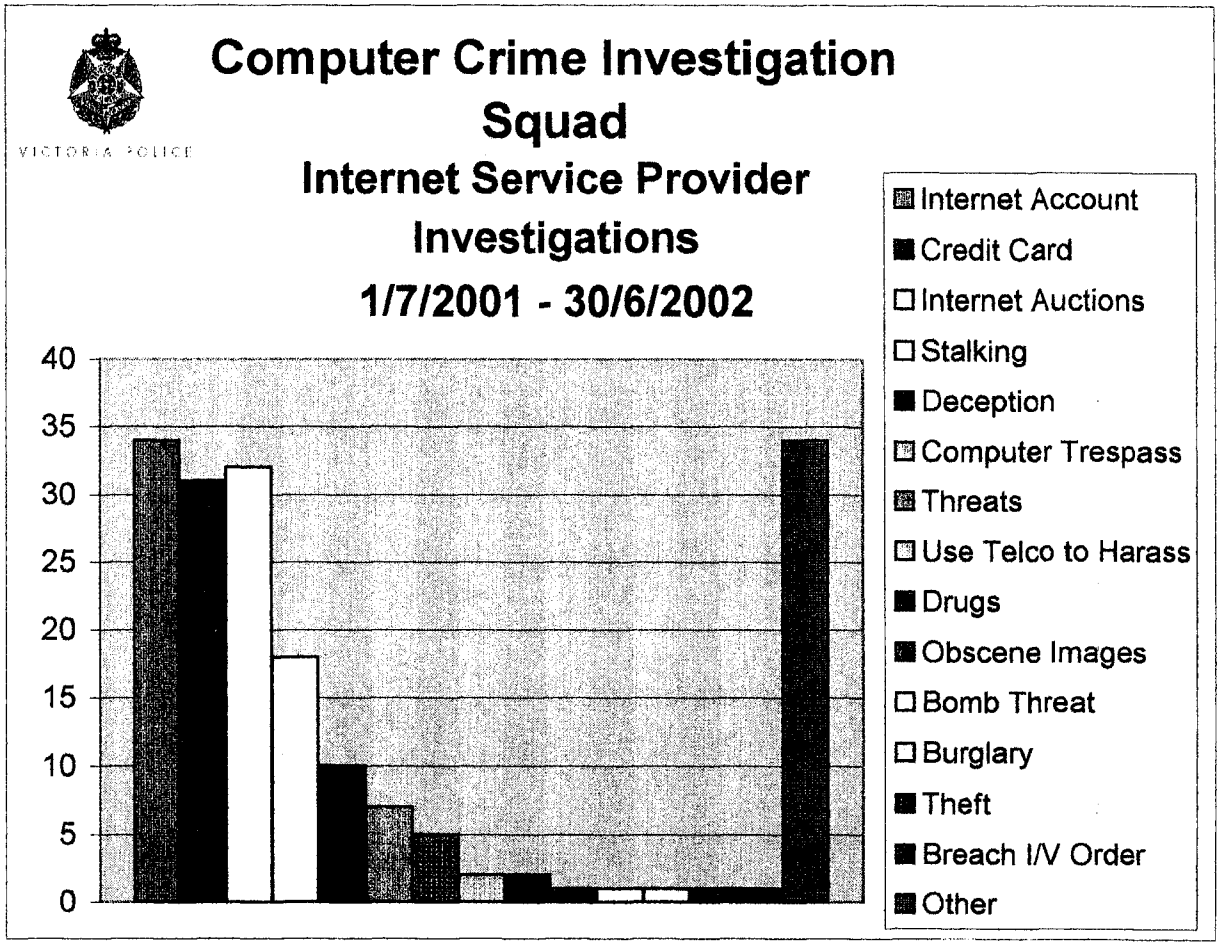
VICTORIA POLICE

Computer Crime Investigation Squad
Drug Analysis Investigations
Financial Year Comparison



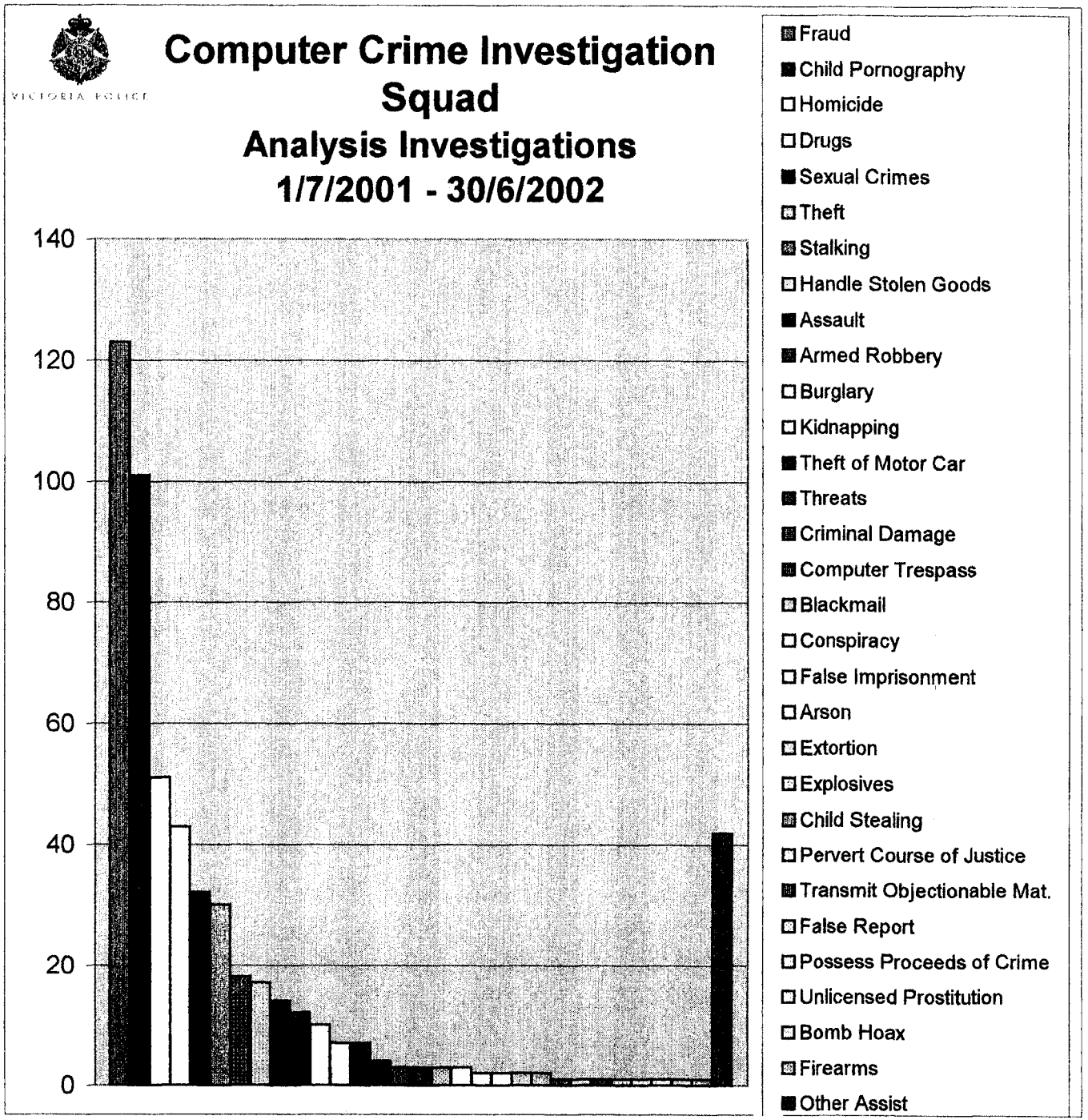
Peter Wheeler
Detective Senior Sergeant 22088
Officer in Charge - Computer Crime Investigation Squad

Internet Account	34	19%
Credit Card	31	17%
Internet Auctions	32	18%
Stalking	18	10%
Deception	10	6%
Computer Trespass	7	4%
Threats	5	3%
Use Telco to Harass	2	1%
Drugs	2	1%
Obscene Images	1	1%
Bomb Threat	1	1%
Burglary	1	1%
Theft	1	1%
Breach I/V Order	1	1%
Other	34	19%
	180	**100%**



Peter WHEELER
Detective Senior Sergeant 22088
Officer in Charge - Computer Crime Investigation Squad

Fraud	123	22.82%
Child Pornography	101	18.74%
Homicide	51	9.46%
Drugs	43	7.98%
Sexual Crimes	32	5.94%
Theft	30	5.57%
Stalking	18	3.34%
Handle Stolen Goods	17	3.15%
Assault	14	2.60%
Armed Robbery	12	2.23%
Burglary	10	1.86%
Kidnapping	7	1.30%
Theft of Motor Car	7	1.30%
Threats	4	0.74%
Criminal Damage	3	0.56%
Computer Trespass	3	0.56%
Blackmail	3	0.56%
Conspiracy	3	0.56%
False Imprisonment	2	0.37%
Arson	2	0.37%
Extortion	2	0.37%
Explosives	2	0.37%
Child Stealing	1	0.19%
Pervert Course of Justice	1	0.19%
Transmit Objectionable Mat.	1	0.19%
False Report	1	0.19%
Possess Proceeds of Crime	1	0.19%
Unlicensed Prostitution	1	0.19%
Bomb Hoax	1	0.19%
Firearms	1	0.19%
Other Assist	42	7.79%
	539	**100.00%**



Peter WHEELER
Detective Senior Sergeant 22088
Officer in Charge - Computer Crime Investigation Squad

PROCLAMATION LAW MEMO

Learning Resource Development Unit
Victoria Police Training Academy
Ph: 9566 9683
Fax: 9566 9576
E-mail: procord@corplink.com.au

Proclamation Memo No. 01/03

Date: **12th May, 2003**

Re: **Introduction of the *Crimes (Property Damage and Computer Offences) Act 2003***

Introduction

The *Crimes (Property Damage and Computer Offences) Act 2003* came into operation on 7th May, 2003. The main purpose of this act is to

- amend the *Crimes Act 1958* to create offences relating to bushfires, computers and sabotage; and
- amend the *Bail Act 1977* to include the offence of arson causing death as one where the court must refuse bail unless the defendant can "show cause" as to why bail should be granted.

Crimes Act amendments

Intentionally or recklessly causing a bushfire

A new offence has been created which makes it an offence for a person to-

- intentionally or recklessly cause a fire; and
- be reckless as to the spread of the fire to vegetation on property belonging to another person.

Section 201A(1)

A person will not be taken to be reckless as to the spread of the fire where the person -

- caused the fire in the course of carrying out a fire prevention, fire suppression or other land management activity; **and**
- carried out that activity in accordance with a provision made by an Act or a Code of Practice; **and**
- honestly believed that his/her conduct in carrying out that activity was justified having regard to all the circumstances.

Computer offences

A number of new offences relating to computer crime have been included in the Crimes Act.

- Unauthorised access, modification or impairment with intent to commit serious offence - section 247B
- Unauthorised modification of data to cause impairment - section 247C
- Unauthorised impairment of electronic communication - section 247D
- Possession of data with intent to commit serious computer offence - section 247E
- Producing, supplying or obtaining data with intent to commit serious computer offence - section 247F
- Unauthorised access to or modification of restricted data - section 247G
- Unauthorised impairment of data held in computer disk, credit card or other device - section 247H

The definitions and full details of all these offences can be found in the Crimes Act at section 247 however members should seek advice from the Computer Crime Investigation Squad on 9865 2757 in relation to any matter involving computer crime.

Sabotage

These amendments have created 2 new sabotage offences.

- Sabotage - section 247K
- Threats to sabotage - section 247L

The amendments provide a number of detailed definitions relating to these offences but put simply these offences relate to a person causing damage or making a threat to cause damage to a public facility by committing a property offence or by causing an unauthorised computer function with the intention of causing

- major disruption to government functions, or
- major disruption to the use of services by the public, or
- major economic loss.

For full details of these offences and definitions of 'property offence', 'public facility', 'unauthorised computer function' and 'damage' see section 247J-247L of the Crimes Act.

Transitional Provisions

These amendments only apply to offences alleged to have been committed on or after the commencement of this Act.

Bail Act amendments

Section 4(4) of the Bail Act 1977 has been amended to include the offence of arson causing death which means that the court shall refuse bail where an accused is charged with arson causing death unless the person can "show cause" as to why his detention in custody is not justified and bail should be granted.

Transitional Provisions

These amendments to the Bail Act 1977 only apply to a charge for an offence filed on or after the commencement of this Act.

Magistrates' Court Act amendments

This Act makes consequential amendments to the Schedule 4 of the Magistrates' Court Act 1989 to provide that the following offences are indictable offences that may be heard and determined summarily.

- Unauthorised access, modification or impairment with intent to commit serious offence - section 247B
- Possession of data with intent to commit serious computer offence - section 247E
- Producing, supplying or obtaining data with intent to commit serious computer offence - section 247F

Summary Offences Act amendments

The offence of gaining access to a computer system or part of a computer system without lawful authority at Section 9A of the Summary Offences Act has been repealed. This offence has been replaced by the new computer offences outlined in section 247B-247H of the Crimes Act.

Further details

The amended Act can be accessed via the Intranet under Victorian Legislation.

Australasian Identity Crime Policing Strategy 2003 - 2005

Introduction

'Identity crime' is a broad term used to describe offences in which a perpetrator uses a false identity, or a real identity other than their own identity ('identity theft'), in order to facilitate the commission of a crime. Identity crime can underpin and facilitate a range of crimes including people smuggling, drug trafficking, money laundering, paedophilia, terrorism and murder, but is most commonly typified by 'identity fraud'.

Police Commissioners, recognising the importance of the issue, developed this Strategy which was launched in March 2003. The purpose of the Strategy is:

To prevent and reduce identity crime and to assist the victims of 'identity theft'.

This Strategy should be used as a companion to the *Electronic Crime Strategy* given that current trends indicate that the preferred medium for the commission of identity crimes is electronic.

Strategy Architecture

In recognising that one approach will not suit all agencies and that agencies may have differing priorities, the key activities are written at a strategic level. Underpinning the Strategy will be an Australasian workplan that identifies specific areas or issues for action. Due to individual jurisdictional resourcing issues and varying priorities, it is recognised that implementation progress within Australasian police agencies may vary.

Strategy Focus Areas

The Identity Crime Strategy has six focus areas that identify what police will concentrate on over the initial two years. The focus areas are inextricably linked and will have limited impact unless dealt with collectively. The focus areas are: Prevention; Victim Assistance; Partnerships; Education and Capability; Resources and Capacity; and Regulation and Legislation.

1. Prevention

Objectives:

1.1 Actively identify and promote preventative strategies and opportunities for organisational target hardening.

1.2 Contribute to sound research and maintain accurate statistics on identity crime by supporting and contributing towards a range of initiatives.

1.3 Produce timely and accurate strategic assessments and intelligence about identity crime trends and activities.

1.4 Consider the problem of identity crimes as multi-jurisdictional, and adopt and enhance appropriate structures within the various Australasian police jurisdictions to address the problem.

1.5 Explore opportunities for research into the application of technology as an aid to detect, prevent and investigate identity crime.

2. Victim Assistance

Objectives:

2.1 Recognise a new class of victim that is emerging as a result of identity theft offences.

2.2 Put in place processes that assist victims of identity theft and provide them with timely and easily accessible advice.

3. Partnerships

Objectives:

3.1 Establish and maintain effective working relationships with international, regional and local law enforcement, government and private agencies.

3.2 Utilise partnerships to educate private and public sector organisations about risks and solutions and to promote processes more resistant to identity crime.

3.3 Develop strong links with key organisations that are involved in Proof Of Identification (POI) processes including financial institutions and other key document providers, in order to improve validation and verification processes.

3.4 Develop and maintain partnerships with communities, interest groups and non-government organisations.

4. Education and Capability

Objectives:

4.1 Provide training to police personnel in order to deal with identity crime issues.

4.2 Create a safer community by contributing to community education about identity crime, and how best to avoid victimisation.

4.3 Utilise the media to increase awareness and educate the community at large in relation to aspects of identity crime.

5. Resources and Capacity Building

Objectives: *Australasian Police to:*

5.1 Have the resources and the enforcement capacity to prevent, respond, investigate and, where appropriate, prosecute identity crime.

5.2 Have sufficient resources, personnel and infrastructure to provide the capacity to respond to multi-jurisdictional and international identity crime investigations.

5.3 Have access to the best intelligence product available relative to identity crime and to recognise a need to improve and enhance current intelligence structures and to supplement with alternative frameworks if indicated.

5.4 Examine emerging technology and, where appropriate, promote its use in both the investigation of identity crimes and in its application to risk management processes within public and private sector organisations.

6. Regulation and Legislation

Objectives:

6.1 Contribute to debate on legislative reform aimed at creating a more effective regulatory and legislative environment across all Australasian jurisdictions in relation to identity crime.

6.2 Work with key stakeholders to achieve a more effective POI regime.

6.3 Examine legislative and regulatory solutions to the identity crime problem in conjunction with key partners who share an interest in the same issues.

The Strategy will provide a useful vehicle to engage the community, other government agencies as well as the private sector, in addressing this complex issue.

A full copy of the Strategy can be obtained from the Australasian Centre for Policing Research website at www.acpr.gov.au

15 May 2003

Interpol media release

15 May 2003

Major child pornography operation broken in Sweden.
Joint effort by Interpol, Swedish and Norwegian police.

NOORDWIJK, Netherlands - Police in Sweden have broken a major child pornography operation after a lengthy joint effort involving Interpol and Norwegian investigators, Interpol officials announced on Thursday.

A series of police raids on residences in Stockholm on May 13 led to the arrest of a man suspected of producing the most sought after series of child pornography images available to collectors of such material, Interpol officer Hamish McCulloch said during Interpol's annual European Conference. Social workers and crisis counselors have already interviewed 15 children thought to be victims and this number could rise to 40, he said.

The pornographers produced some images to order for collectors.

'This was a very complex case and the production of these pornographic images, a series often using the same children, had been going on for more than five years,' Mr McCulloch said. 'The investigation, which used Interpol's child pornography database and sophisticated image analysis, allowed Norwegian police, and then police in Sweden, to break up the operation and make the key arrest.'

Interpol in 2001 provided Norwegian police with approximately 1,500 images from its extensive image child pornography database and Norway then assigned officers to follow up on Interpol's analysis. Technical examination of such things as vegetation and rock formations in outdoor scenes allowed investigators to narrow down their search for the region where the images were being produced.

A breakthrough after analysis of computer and Internet data led to the Stockholm raids this week.

'This is an excellent example of how Interpol information and analysis enhances international police cooperation and leads to arrests,' said Anders Persson, a Swedish police officer seconded to work at Interpol's General Secretariat in Lyon.

Interpol has been stepping up its investigation and analysis of child pornography images since 1997. Its database of some 150,000 photographs allows police around the world to compare images and make important links between locations, images and photographic styles.