SENATE STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS
AUSTRALIAN FEDERAL POLICE

Question No. 100

Senator McKenzie asked the following question at the hearing on 24 May 2012:

a) How do you define cybercrime?

b) What is the agency's budget for tackling cybercrime? How is this broken down?

c) How many staff does the agency devote to tackling cybercrime? How is this broken down? Where are these staff physically located? What are they working on?

d) What performance indicators have been set around cybercrime?

e) What work is being undertaken in relation to cyber crime and liaising with the community?

The answer to the honourable senator's question is as follows:

a) The AFP endorses the definition of cyber crime used by the Australia New Zealand Policing Advisory Agency (ANZPAA) e-Crime Committee (AeCC) which was signed off by all of the Commissioners.

Cybercrime is defined as:

- crime directed at computing and communications technologies themselves, such as unauthorised access to, modification or impairment of electronic communications or data

- crime where the use of the internet or information technology is integral to the commission of the offence, (sometimes referred to as a technology-enabled crime) such as online fraud (eg internet or email scams), online identity theft, online child exploitation and online intellectual property infringement.

It does not include crime where the use of the information technology is incidental to the commission of the offences.

b) The agency's budget for tackling cyber crime for 2011-12 financial year is: $20,965,000

It can be broken down by:

Human resources costs	$15,236,000
Capital Costs	$ 2,394,000
Operating and maintenance costs	$ 3,335,000

Total

Human resources costs	$15,236,000
Capital costs	$2,394,000
Operating and maintenance costs	$3,335,000
Total	$20,965,000

Cyber Crime Operations

Sub-total of Human resources costs	$2,071,000
Capital costs	
Operating and maintenance costs	$434,000
Total	$2,505,000

Child Protection Operations

Human resources costs	$4,245,000
Capital costs	
Operating and maintenance costs	$921,000
Total	$5,166,000

Crime Program

Human resources costs	$259,000
Capital costs	
Operating and maintenance costs	$70,000
Total	$329,000

CFT

Sub-total of Human resources costs	$7,811,000
Capital costs	$2,394,000
Operating and maintenance costs	$1,728,000
Total	$11,933,000

Crime prevention

Sub-total of Human resources costs	$850,000
Capital costs	
Operating and maintenance costs	$182,000
Total	$1,032,000

c)

The AFP continues to invest significant resources and effort into our cyber capabilities. Whilst the High Tech Crime Operations function represents our primary cyber response, the nature of cyber crime and the pervasiveness of technologies through the myriad of crime types mean that the AFP now has an organisation wide focus on cyber capability.

Areas of the AFP that have quite specific cyber related roles, responsibilities and resourcing are Child Protection Operations, Cyber Crime Operations, Cyber Crime Prevention, Crime Program (representing our Serious & Organised Crime and Crime Operations functions) and the Computer Forensic Team (within our Forensic & Data Centres function).

The total number of staff devoted to cybercrime is provided below.

Cyber Crime Operations	17
Child Protection Operations	51
Computer Forensic Team	57
Crime Prevention	7
Total	**132**

Further to these statistics, it is important to realise with the AFP's functional model we have the capacity for surge members if required. A good example of this relates to Child Protection Operations where between 1 July 2011 to 30 April 2012, a total of 82,638 hours were expended on Incident Types related to Child Protection Operations (CPO) (47,344 hours of which were attributed by HTCO). A total of 421 members from across the AFP (97 from HTCO) contributed to these hours.

Canberra office hosts the majority of HTCO members, however with members in all AFP offices both domestically and internationally the AFP has enhanced capability to address cybercrime and a centrally coordinated high-technology operations support function.

High Tech Crime Operations (HTCO) provides the AFP with an enhanced capability to investigate, disrupt and prosecute offenders committing serious and complex technology crimes. HTCO monitors trends of cybercrime and participates in intergovernmental and international forums with national and international strategic partners.

HTCO aims to build a highly technical investigative capability for the AFP to anticipate and identify emerging technology challenges for law enforcement and to develop response strategies to these by engaging with domestic and foreign law enforcement agencies, government, industry, academia and the public. The following provides a breakdown of what the areas are working on.

Child Protection Operations

In combating transnational and online child sexual exploitation, the AFP has forged strong relationships with national and international law enforcement communities. In collaboration with its international partners, the AFP has successfully identified and charged numerous offenders for child sexual exploitation offences. Child Protection Operations teams continue to work collaboratively with foreign law enforcement professionals to combat child sex tourism. This includes the active monitoring and prosecution of child sex offenders. As part of the strategy-based approach, Child Protection Operations is developing proactive measures to combat child sex tourism. These strategies include deployments to targeted jurisdictions to map the environments and build stronger relationships with local law enforcement and non-government organisations.

Cyber Crime Operations comprises investigators and technical experts dedicated to investigating and prosecuting computer crimes under the Commonwealth Criminal Code Act 1995, including:

- significant computer intrusions and related offences such as
- breaches of corporate or government computer systems
- collective large-scale breaches of individual computer systems in homes or businesses to harvest personal, business and/or financial data
- creating, controlling or distributing botnets
- creating, supplying, possessing or controlling malicious software with the intent to commit or facilitate serious computer offences
- activities related to those above which directly impact the banking and finance sector (including phishing, 'mule' recruitment and online criminal trading of financial, business and/or personal data).

The teams also closely collaborate with system owners from both government and the private sector to protect the security and stability of Australia's critical information systems and its burgeoning digital economy through proactively mitigating cyber threats.

Through the Cyber Crime Operations teams the AFP provides a national law enforcement investigative capacity in accordance with the government's Cyber Security Strategy. As an active partner of the Cyber Security Operations Centre and CERT Australia, the AFP continues to implement intelligence-led policing methods of identifying and mitigating cyber security events through enhanced intelligence sharing opportunities.

HTCO Crime Prevention develops and implements crime prevention strategies through heightened education and awareness, recognising the importance of education in combating cybercrime. The Crime Prevention Team has been instrumental in implementing strategies aimed at raising awareness of online risks and empowering online users to protect themselves online.

As cyber safety and security is everybody's responsibility, the team has fostered relationships with government and non-government organisations, industry and community groups to ensure key cyber-safety messages reach their intended targets.

Crime Program

Through the Crime Operations Portfolio, cybercrime investigations include those that involve fraud, information and communication technology, intellectual property and in some instances, identity crime.

Computer Forensic Team

- The AFP Computer Forensics Team provides an operational support service to AFP National Operations and ACT Policing, as well as other government and law enforcement agencies.
- The team specialises in obtaining, analysing and presenting electronic evidence stored on computers and other electronic devices. In this capacity, the Computer Forensic Team provides

integral support to AFP cybercrime investigations, particularly investigations conducted by AFP Child Protection Operations and Cyber Crime Operations.

- The Computer Forensics Team is staffed in Brisbane, Sydney, Melbourne, Perth and Canberra and operates accredited laboratories in these locations. Common services provided by the team include:

    - On-site identification, examination and preservation of electronic evidence at crime scenes and during search warrant execution
    - Laboratory examination of digital devices and electronic evidence
    - Electronic data recovery, password recovery and data decryption
    - Court attendance to give factual and expert evidence as a forensic practitioner.

d) What performance indicators have been set around cybercrime?

For High-Tech Crime, the performance indicators set around cyber crime investigations are:

- fight cybercrime including online child protection offences and travelling sex offender offences, cyber-security threats and events, and computer and banking offences
- develop and implement child protection offence prioritisation through a review of referral processes
- AFP education and awareness programs
- prevention: external education and awareness programs, and
- strategic deliverables: collaboration with government, industry specialists (including non-government organisations) and academia outreach to combat technology enabled crime.

Key performance indicators	**2010–11 Revised budget**	**2011–12 Budget target**	**2012–13 Forward year 1**	**2013–14 Forward year 2**	**2014–15 Forward year 3**
High-Tech Crime					
Cybercrime investigations					
Percentage of time spent on high to very high impact cases	80%	80%	80%	80%	80%
Number of high to very high impact cases reaching court	60	70	80	90	90
Percentage of cases before court that result in conviction	90%	90%	90%	90%	90%
Percentage of AFP personnel having completed technology-related (Tier 1) training	20%	40%	60%	80%	85%
Enhanced community awareness of cybercrime (% of surveyed sample indicating increased awareness or reinforcement of awareness post delivery of presentations)	80%	80%	85%	85%	85%

Note: The indicator for the level of internal client/stakeholder satisfaction has been removed as its primary usefulness was as an internal AFP measure. The level of external satisfaction remains through the business satisfaction survey.

e)

In March 2008 HTCO established a dedicated crime prevention team to develop and implement crime prevention strategies through heightened education and awareness. This innovative approach recognises the importance of prevention through education in combating technology crime.

The crime prevention team has been instrumental in implementing strategies aimed at raising awareness of online risks, empowering all online users to protect themselves online.

As cyber safety and security is everybody's responsibility, the crime prevention team has fostered relationships with government and non-government organisations, industry and community groups to ensure key cyber-safety messages reach their intended targets – the Australian community.

Crime Prevention Awareness Campaigns

ThinkUKnow

ThinkUKnow cyber-safety program is aimed at bridging the knowledge gap that exists between adults and young people when it comes to the internet and mobile technologies and to encourage a more open dialog between them.

ThinkUKnow is a partnership between AFP, Microsoft and is proudly supported by ninemsn, and now Datacom.

ThinkUKnow has used a trained network of volunteers from partner organisations to deliver awareness-raising sessions to parents, carers and teachers across Australia to protect them and what to do if things go wrong. The presentation covers cyber bullying, sexting, online grooming, scams, identity theft and other issues and is supported by online resources through our website ThinkUKnow.org.au.

During 2011, 134 presentations were delivered to 4383 Parents, Teachers and Carers. There were also 3468 members on the ThinkUKnow website at 1 December 2011. There have been over 49,719 hits on the ThinkUKnow website this year and 922,014 visits to the ThinkUKnow Youtube site since 12 November 2009.

Cyber Safety

AFP cyber safety presentations are delivered to young people aged primarily between 11 and 18. These presentations seek to educate children on the risks they can encounter online, exploring issues such as sexting, cyber bullying, social networking, digital footprints and the importance of protecting their reputations. Importantly we develop solutions for what children can do to protect themselves and what to do if things go wrong. During 2011 the AFP delivered 156 presentations to 22,385 young people. For 2012 to 31 May the AFP have delivered 75 presentations to 8,818 young people.

In addition, the Crime Prevention Team delivered 44 online reputation management seminars to 1,713 professional sporting teams and NRL junior teams.

Social Media & Reputation Management

AFP Social Media & Reputation Management presentations are delivered to elite athletes and professional sporting groups (athletes, training staff and their executive officers) highlighting the benefits and vulnerabilities of social networking, raising awareness of their own digital footprint and discussing mechanisms and methodologies to protect themselves and their identify online. The initiative follows a similar model as the Illicit Drugs in Sport framework encouraging sports men and women to become positive roll models in the community. The presentations are also delivered to AFP recruits entering the organisation. During 2011 the AFP delivered 44 presentations to 1713 young athletes. For 2012 to 31 May the AFP have delivered 20 presentations to 1135 athletes

Cyber Safety Pasifika

Use of the internet in the Pacific is growing, particularly among children and young people. While ICT skills are being taught in many schools, very little attention is given to safety and security online.

Cyber Safety Pasifika is a crime prevention initiative whose pilot program is being delivered to four countries through the Pacific Island nations, including Tonga, Micronesia, Niue, Samoa and Cook Islands. Training of officers from those countries was held in early Feb 2012. The initiative also includes the establishment of a Cybersafety Pasifika website.

The program seeks to educate at risk communities in the Pacific on cyber safety issues such as protecting your identity, sexting, cyber bullying, online grooming and e-crime; improving the digital literacy of communities new to social networking and the internet. This program is an initiative of the Pacific Islands Chiefs of Police Secretariat, of which the Australian Federal Police is represented.

Northern Territory Police

Crime Prevention members have recently delivered a number of Internet Safety presentations to children, parents and carers living in Darwin, Alice Springs and several remote indigenous communities. This has been part of the Northern Territories Department of Justice Stronger Choices Program.

This has created demand for further Internet safety presentation throughout the Northern Territory. As a result, the AFP has drafted a MoU with Northern Territory Police (NTPOL) in the provision of cyber safety initiatives.

This will enable further training of NTPOL members in the delivery of ThinkUKnow and school internet safety programs, as well as the provision of collateral support to the presentations.

Having a larger capacity with the NT will improve the HTCO Crime Prevention ability deliver such sessions in the Northern Territory. This will allow as many people as possible, including future generations in the NT remote community's access to important Internet safety information.