Leading the charge on technology-led policing

By Anne Quinn

From left: Assistant Commissioner Andrew Colvin with HTCO members Dr Jenny Mouzos, Ian Wilson, Federal Agent Reece Kershaw and Jess Negus.

High tech crime is no longer new but the criminal mind continues to seek new ways of exploiting 21st century technology. A generation has now grown up online experiencing both the bane and benefit of this modern double-edged sword. The AFP has kept pace as the criminal patterns evolve and is now suiting up for the next level of battle.

National Manager of High Tech Crime Operations (HTCO), Andrew Colvin, is responsible for a 'new' function within the AFP that is dedicated to investigating technology-related activities in Australia and overseas. HTCO was established in March 2008 and represents the integration of various AFP units, including the Australian High Tech Crime Centre, Online Child Sex Exploitation teams, cyber-safety teams (formerly Protecting Australian Families Online) and Technical Operations.

Assistant Commissioner Colvin's vision for 2012 is that the AFP will be technically adept, comfortable with technology and its applications, and poised to exploit every bit of technology to its fullest capacity.

"The AFP has recognised the importance of building its capacity and capabilities in response to the growing challenges of technology-enabled activities and in particular online crime," Assistant Commissioner Colvin said. "It has also identified the need to centrally coordinate high tech support to ensure these environments are properly policed."

While the HTCO function includes areas such as child protection and high tech investigations, Assistant Commissioner Colvin is keen to highlight it is just a new way of doing 'old' business.

"We are about finding solutions for all crime types. We will focus on innovative use of technology to provide support to all functional areas of the AFP," he said. "Just like intelligence and forensic services—we are an enabler of the organisation."

Internet policing

A generation of adults now entering the workforce has never known a world without the information superhighway.

From communication advancements including wireless internet access, iPhone and BlackBerry— to new forms of social networking like *MySpace* and virtual gaming websites like World of Warcraft— the virtual world is a strange and unfamiliar place to many who are not Generation Y.

From a crime-fighting perspective, the AFP has recognised that the internet provides a new platform for committing old crimes. Commissioner Keelty explains:

" ... the internet has four key attributes that make it ideal to commit a crime: it has global connectivity, it provides anonymity ... it provides a lack of traceability in a lot of cases and it provides a world full of valuable targets."

HTCO has established a new team within the Innovation and Prevention stream dedicated to covert online investigations and disrupting the new areas that internet criminals are currently exploiting or likely to use in the future.

One of the team leaders Federal Agent Richard Chin explained the work they do is performed for any function of the AFP.

"We proactively assist the AFP's child protection operations and have had good successes with jobs related to grooming and procuring as well as identifying child sex offenders who are actively involved in illegal trading of child exploitation images and/or material," Federal Agent Chin said.

In July 2008 following a three-month investigation by the AFP's Internet Policing Team (IPT) an Australian man was charged with child pornography offences. While the crime was not new, the methodology used by the AFP involved the use of covert identities to gather evidence of the man's criminal activities.

Another spin-off success story for the IPT has been the recent prosecution of a US citizen who was imprisoned for 40 years for trading in child pornography.

"Through our close relationship with the FBI we referred information about the offender which assisted greatly in the FBI's investigation," said Federal Agent Chin. "In the past 12 months we have referred more than 100 offenders to law enforcement agencies around the world and have been able to cross borders as effectively as the criminals who use the net."

Social networking

Assistant Commissioner Colvin explained online communities, commonly known as 'social networking', have also changed the way that people communicate and police investigate.

"The internet has created an environment where Generation Y communicates in a virtual world via social networks such as *Facebook*. These environments provide users with fun social outlets as well as learning environments that allow information, ideas and research discussions to occur in chat rooms at a pace unlike any communication revolution before.

"Criminals have also identified these social networking sites as places to meet and plan crimes," said Assistant Commissioner Colvin.

In late 2006 the US National Cyber Security Alliance (NCSA) conducted research into users of social networking sites and found that 74 per cent of users divulge personal information such as their email address, name and date of birth. It also revealed that 83 per cent of users downloaded unknown files from other people's profiles that could potentially lead to identity theft or other threats such as fraud, computer spyware and viruses (Source: NCSA Media release 4 October 2006).

Partnerships with industry

Earlier this year the AFP forged an innovative partnership with Microsoft. It is the first time police and software developers have led the way in harmonising policing and technological development. Assistant Commissioner Colvin explained that Superintendent Mick Kelsey is working with Microsoft to be at the forefront of cyber development and any emerging trends.

"No other law enforcement agency in the world has placed a senior member into such a role," Assistant Commissioner Colvin said. "This positioning was achieved through Microsoft understanding that the AFP is approaching these issues differently and is focused on working with industry to achieve a positive outcome for the community."

Commissioner Keelty also believes the partnership with Microsoft will be visionary in terms of where they are going to take the next level of cyber development.

"I think these sorts of relationships are the way of the future for policing. Where once upon a time policing was a bit reticent to partner with the private sector," Commissioner Keelty said.

In August 2008 the AFP partnered with *MySpace* and *YouTube* to promote National Missing Persons Week. The AFP decided that reaching young people about an important issue required a modern approach and going online to engage them in their virtual world.

Vice-President of Fox Interactive Media Ms Jennifer Mardosz believes internet safety is a top priority for *MySpace* and joining forces with law enforcement is an important part of user safety online.

"We're pleased to partner with the AFP and appreciate the innovative approach the organisation is taking to protect children online," Ms Mardosz said.

Academic outreach

Coordinator for HTCO's Crime Prevention Dr Jenny Mouzos is leading the team on a range of new initiatives.

"The AFP is funding and establishing partnerships with a range of academic institutions in order to remain at the forefront of knowledge and technological advancements," Dr Mouzos said.

The AFP is a key partner of the Centre of Excellence in Policing and Security—an initiative established by the Australian Research Council (ARC). The Centre, launched earlier this year, has received $26 million from the ARC to research policing and the security sector.

Current projects relevant to HTCO include PhD research into offenders and criminal justice and regulatory responses to 'cyber-predation'—the latter focuses on men and women who use the internet to groom and lure minors for sexual gratification. Another project seeks to examine the criminal exploitation of new and emerging technologies including internet, mobile phones or any combination of both. The outcomes of both of these projects will benefit portfolios across the AFP and ultimately the broader community.

Griffith University Vice-Chancellor Professor Ian O'Connor said the Centre's world-class scholars would expand Australia's understanding of transnational security threats and help build new responses to the security challenges of the 21st century.

"The $32 billion per year national cost of crime and the pervasive nature of terrorism in the post-September 11 environment creates a real and urgent need for high-quality research of a scale, focus and depth not previously undertaken in Australia," Professor O'Connor said.

Recently the AFP provided funding to the Internet Commerce Security Laboratory (ICSL)—a joint venture between the University of Ballarat, the Westpac Banking Corporation, IBM Australia and the Victorian Government.

ICSL will focus on two approaches to addressing cybercrime by profiling the activities of criminal groups and developing technologies to ensure consumers can use internet commerce with confidence. It will also target identity theft, viruses, worms, malware, financial fraud and spyware, and develop solutions to identify organised cyber criminal groups around the world.

International Youth Advisory Congress

In July 2008 more than 150 young people aged 14 to 17 from around the world, including 10 representatives from Australia, attended the International Youth Advisory Congress (IYAC) in London. Delegates discussed issues in break-out sessions and then presented strategies to representatives from government, industry, law enforcement, education and media.

The outcomes from IYAC will be presented in November to the World Congress III against Sexual Exploitation of Children and Adolescents to be held in Brazil. Two IYAC youth delegates will attend the World Congress and present recommendations that will later form the basis of the Children and Young Persons Global Online Charter.

The Charter will form part of the submission to the UN Convention of the Rights of the Child in accordance with article 12 of the Convention which relates to giving children a voice in issues that affect them. The submission aims to amend article 34 to address the advent of technology as an important part of children's lives.

The Charter will also be used to inform the crime prevention activities of HTCO,

Above: In 2007 Foxtel's Crime and Investigation Network aired a Virtual Global Taskforce television community service announcement to promote cyber safety and show how the police are tackling online crime.

Left: Commander Kevin Zuccato with Australian delegates at the International Youth Advisory Congress held in London earlier this year.

which focuses predominantly on raising awareness of technology-enabled crime, and educating children, parents, teachers and the general public on how they can protect themselves online.

A tech-savvy AFP

Assistant Commissioner Colvin believes the IPT is a shining example of technology-led policing that is already benefiting other areas of the AFP.

"From money laundering and banking fraud to Intellectual Property and copyright offences and counter terrorism HTCO is providing advice, training and new strategies to assist investigators to understand and embrace the internet and new technologies," Assistant Commissioner Colvin said.

HTCO is also taking up the challenge to improve AFP members' awareness of technical developments in the facilitation of crime, including terminology, trends, modes of communication and basic awareness of software and hardware components.

Technology has historically been a double-edged sword—it can be manipulated for good or evil. To combat highly adaptive criminals, HTCO will remain at the core of an increasingly tech-savvy police force waging a constant battle against the world of technology-enabled crime.

Above: Delegates at the International Youth Advisory Congress deliver their presentations to various sector representatives.

AFP and Interpol: Fighting high tech crime in South America

The AFP's growing international reputation in fighting high tech crime was illustrated recently when the organisation was invited to assist Colombian authorities in a major operation.

In March 2008 Colombian police retrieved eight computer devices during a raid on a Revolutionary Armed Forces of Colombia (FARC) rebel base near the Colombian–Venezuelan border.

In response to a request from Interpol, an AFP computer forensic expert was seconded to the Interpol Response Team (IRT) to assist in the investigation, along with an expert from the Singapore Police Force.

In May Interpol announced in a media release:

"The IRT determined the eight seized computer exhibits contained more than 600 gigabytes of data, including:

- 37,872 written documents
- 452 spreadsheets
- 210,888 images
- 22,481 web pages
- 7989 email addresses
- 10,537 multimedia files (sound and video)
- 983 encrypted files.

In non-technical terms, this volume of data would correspond to 39.5 million filled pages typed in Microsoft Word and, if all of the seized data were in Word format, it would take more than 1000 years to read at a rate of 100 pages per day.

Details of this operation are contained in a public report Interpol's Forensic Report on FARC computers and hardware seized by Colombia released in May 2008.

The report is available at: <www.interpol.int/Public/ICPO PressReleases/PR2008/pdfPR200817/Default.asp>.