High Tech Crime: AFP casts a wide Net

Imagine the world before computers.

Police would spend hours at the scene of a crime. They would interview witnesses and take statements. They would wearily go into the office and compile their report using an ancient hammer-strike typewriter where the keys would clog together. If they made a mistake they could use liquid paper, but on some legal documents they would have to start again.

There was no email, so carbon paper was placed between typing sheets to provide multiple copies of a document. It was a long, slow, process.

In 1984, the arrival of a fax machine for the AFP's officer-in-charge of the Interpol Bureau in Canberra was so significant that photographs were taken of him showing it to a representative from the Thai police.

By 1990, the AFP had started to use personal computers. Members were trained to use data entry systems, and local area networks were established so that information could be shared between AFP locations.

But it wasn't until 1991 that video and audio recordings were made of police interviews.

Today, the AFP uses some of the most sophisticated computer technology in the world. Members across the globe can access information about cases simply by logging on. Officers are making their presence known on the internet, policing chat rooms and websites to identify and stop those undertaking criminal activity.

Unfortunately, law enforcement agencies aren't the only ones making use of new technologies. Criminals are doing everything they can to avoid detection, and cyberspace has provided them with many new opportunities.

In 2003, the Australian High Tech Crime Centre (AHTCC) was launched and hosted in Canberra by the AFP. The AHTCC provided a nationally coordinated approach to technology enabled crime and its core functions include; policy advocacy, strategic intelligence support, crime prevention and education and capability development. In June 2007, the AHTCC transferred from being a nationally-governed centre to becoming a dedicated AFP portfolio, retaining its national focus. A new High Tech Crime Operations (HTCO) portfolio was officially launched in 2008. HTCO is responsible for investigating online child sex exploitation, liaising with banking and finance institutions to protect them from cyber-attack, protecting Australia's information infrastructure and combating other forms of technology enabled crime.

It has been said that the internet knows no geography. That means law enforcement agencies have to cooperate in new ways to combat the criminals which take advantage of the fluid borders and anonymity of cyberspace.

To this end, the AFP is part of the Virtual Global Taskforce (VGT). Members come from Australia, the UK, Canada, the United States, Italy and Interpol. Non-policing agencies such as Microsoft, the Australian Communications and Media Authority, Visa and BigPond also actively support the VGT. Its aim is to make the internet safer; identify, locate and help children at risk of sexual exploitation; and to hold the perpetrators of online child-sex offences to account.

The AFP has had some significant successes in this area. Over the past two years, more than 300 Australians have been arrested and charged in relation to the online sexual exploitation of children. Several children considered to be at risk were removed from harm. A single operation resulted in the seizure of more than 15,000 videos and more than 500,000 images of child abuse.

One of the issues investigators are trying to deal with is the overwhelming amount of child abuse material on the web. Offenders believe they are anonymous in cyber-space, predators engage in illegal activities thinking they cannot be traced. But organisations like the VGT are helping to ensure this is not the case. Police around the world are determined to stamp out the abuse of children, and are working together more closely than ever before.

A good example is the success of investigations such as the AFP’s Operation Centurion which involved law enforcement agencies in 170 countries. The operation began with an Interpol referral in relation to a website containing images of child abuse. The AFP, with its state and territory counterparts, executed more than 100 warrants in Australia, which led to the arrest of 59 people including school teachers, public servants, accountants, IT professionals and a police officer.

No one accessing illegal material on the internet is immune from prosecution.

The AFP also works with community groups, parents and schools to educate children about staying safe online. The ‘ThinkUKnow’ program is designed to help teachers, carers and parents. It focuses on helping children to develop tools to identify inappropriate or suspicious behaviour online, and gives them advice on what to do if they are approached. Children are also taught how to use the internet in a safe and secure way.

Children are not the only people at risk of becoming victims of cyber-crime. As people around the world make use of the internet for vital communications, e-commerce and banking transactions, criminals will find ways to exploit them. Words like ‘phishing,’ ‘spam’ and ‘spyware’ have all entered the lexicon in recent years, and highlight the extent of the problem.

The AFP’s HTCO is focused on working with the community to prevent, mitigate and disrupt illegal activities online, and actively seeks the community’s support in identifying criminal behaviour. It also works with the banking and finance sector to deal with online fraud, money laundering, scams and identity theft.

New technologies are also helping the AFP to combat more traditional crimes. In cooperation with agencies such as the Australian Tax Office, police can investigate matters such as tax fraud far more effectively than ever before.

Offshore tax evasion schemes have been targeted as part of Project Wickenby. This whole-of-government initiative focuses on investigating and disrupting the use of global tax and secrecy havens for tax evasion and money laundering schemes. The AFP has charged 39 people over this type of activity.

In addition to the work done as part of Project Wickenby, the AFP also targets other forms of tax fraud. In June this year warrants were executed in relation to a $38 million tax-evasion syndicate which allegedly involved Melbourne-based businesses.

Despite the success of this type of operation, police know that to combat cyber-crime they need to develop new technologies to stay one step ahead.

So try to imagine the world in 30 years time.

Police will still spend hours at the scene of a crime. They will still need to make reports. But they will have access to global databanks of information. They will be able to view live feeds of interviews taking place in a different city, or another country. Reports will be updated using voice-recognition software. Technology will enable police to trace evidence in a multitude of ways that haven’t yet been imagined.

But it doesn’t matter how far into the future you travel, Australia’s policing agencies will still be there, working to fight crime of all kinds.