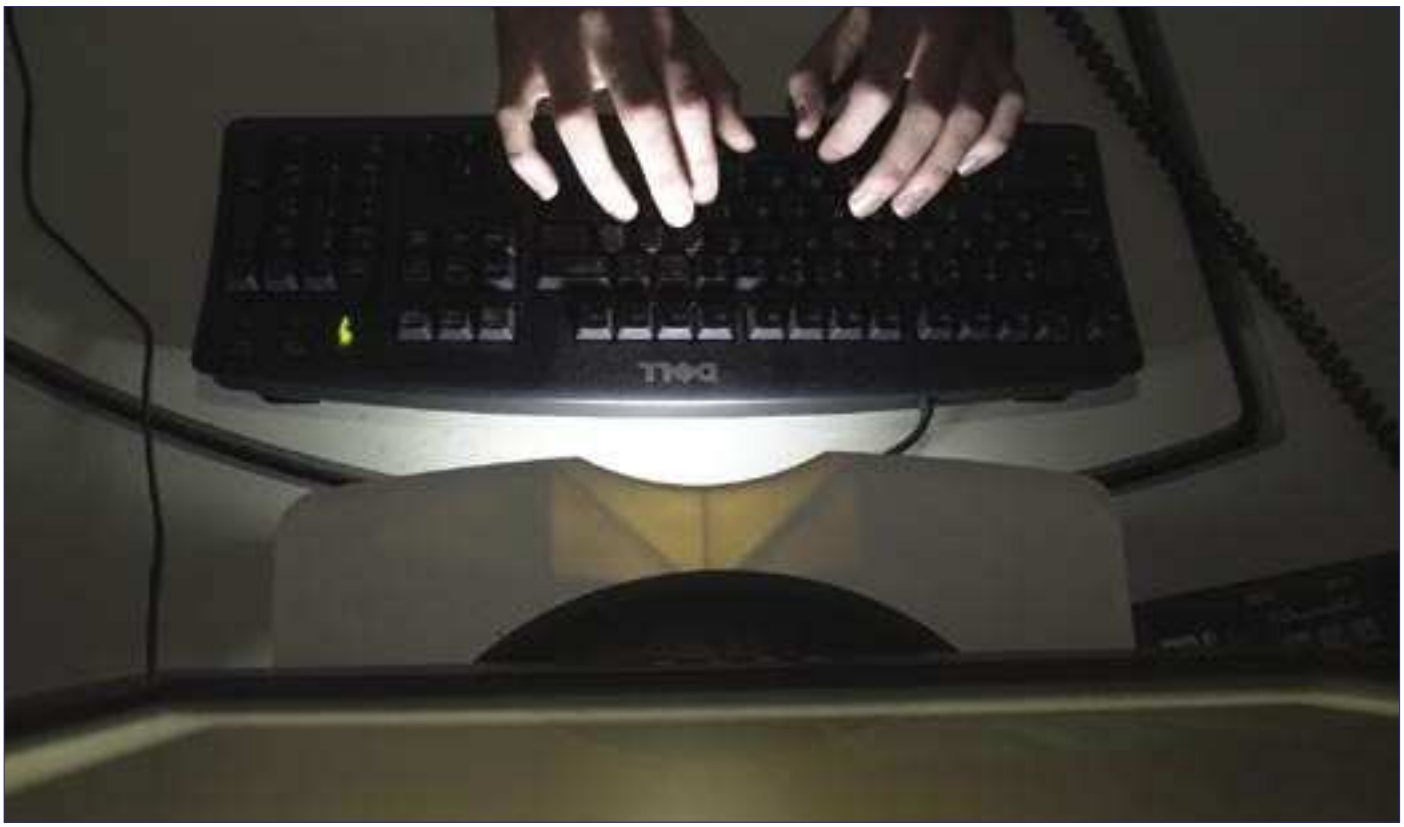
Fighting the invisible



The newly established Australian High Tech Crime Centre (AHTCC) will take the fight against cyber criminals to unprecedented levels.

Based in AFP Headquarters in Canberra, it will bring together experts from the AFP and all State and Territory police services. One of its first challenges will be establishing the extent of electronic crime, according to the centre's Nick Klein.

"One of our big goals is to answer the question of what high tech crime looks like in Australia, because no one really knows the full extent", Klein, a specialist employee, said.

One of the major stumbling blocks has been the under-reporting of high tech crimes, an area already being assisted by the AHTCC's email crime reporting service.

"Police can't respond to matters they don't know about," Klein said.

Perhaps more importantly, police services cannot structure themselves properly for the future if they are unable to assess the environment to which they

are expected to respond, according to AHCTT Director Alastair MacGibbon.

High tech crimes fall into two broad categories. The first, computer enabled crimes, include crimes committed with or against computers, such as hacking, changing data, blocking services or introducing viruses, worms or Trojans. Maintaining a credible assessment and investigative capability in this category is essential for the AHTCC.

According to Federal Agent Brian Diplock, Team Leader of the Computer Enabled Crimes Section, this is an area where specific technical skills are needed, as well as strong support from industry.

"We have been very pleased by the level of technical assistance industry has provided us," Federal Agent Diplock said.

"They possess contemporary knowledge of proprietary systems which we'll never be able to adequately cover."

The second category of high tech crime is computer enhanced crimes, where technology is used to help commit traditional crimes such as fraud, child sexual exploitation, terrorism or money laundering. In these cases criminals use computers to do things such as help plan and coordinate, target victims, move funds, and a range of other functions.

"Criminals have used Internet technologies to target more victims and find willing - if not sometimes unwitting - partners," Federal Agent Nigel Phair, Team Leader of the Computer Enhanced Crimes Section, said.

> We've got operations going at the moment that go across multiple crime types all over the world and it makes it tremendously interesting. We've got a hell of a lot of work to do and we are always learning new things.

"The highly publicised bank 'ghost' websites are a classic illustration: spammed e-mails go out to millions of Australian computer users, hoping that some will use the hyperlink contained in those emails to provide their login and password details to the fraudulent 'bank' site which are then stolen by the criminals.

"The criminals then use the Internet again to find people willing to use their Internet banking accounts to receive funds which they are then asked to convert to cash and remit overseas, less a commission for their troubles.

"It is a deceptively simple scheme, and one which would be possible without the Internet, but not as profitable, and not as geographically diverse."

The AHTCC is structuring itself along these crime type divisions, and growing in size as partner agencies come on board. The strength in the Centre will be the diversity of skills needed to address the staggering array of problems it will face.

Klein is a good example of the expertise in the AHTCC team, with a background in IT audit work.

"I got to look at many different systems, companies and industries all around the word and it was a great way to get a very broad range of experience," he said.

"When the Internet started getting bigger and security started becoming a focus I moved to IT security, which included things like ethical hacking. We would break into computer systems at the request of the system owners, and see how secure they were and would then help them build more secure systems. From there it was a career move to the AFP.

The Liaison Officer Network is the jewel in the crown of the AHTCC.

"While I come from a technical IT security background, we've got people who have spent their careers in national police investigations. We've also got people who have extensive experience in areas like intelligence, surveillance, protection, the bomb squad, and drugs."

Strategic alliances being forged by the AHTCC with international agencies such as the UK's National High Tech Crime Unit and similar organisations in the United States run by the FBI, US Customs and Secret Service give the Centre a reach well beyond Australia. Those alliances are built upon the AFP's International Liaison Officer Network.

"The LO Network is the jewel in the crown of the AHTCC, Federal Agent MacGibbon said.

"We can have enquiries conducted anywhere in the world with minimal bureaucratic overhead and minimal delay; essential in a crime type where criminals are able to jump between jurisdictions without leaving home, and who rely upon the transient nature of computer evidence to hide their tracks."

The AHTCC is also bolstering relationships at home. All Australian Police Commissioners form the Board of Management, with Commissioner Mal Hyde of South Australia holding position of Chair. The New Zealand Police Commissioner sits on the Board in an observer capacity.

A strong relationship with similar units in State and Territory Police Services is the essential ingredient for success. In the next 12 months the AHTCC hopes to build on those links and expand them to other government departments involved in IT security and Internet regulation.

"The only way to project a law enforcement presence on the Internet is together", according to Federal Agent Phair.

"If it is done in an ad hoc fashion we have wasted our time. Together we can make a difference both in Australia and globally. That's what the public expects us to do and we're on the right track."

No single person, agency or corporation holds the key to this. There is no 'silver bullet', just a lot of leg work and a lot of bridge building. We need to do that in Australia and overseas.