



Fact Sheet



October 2004

Australian High Tech Crime Centre

Any crime can be considered 'high tech' when a computer or other piece of technology plays a significant role. This includes crimes committed with or against computers or communication systems, such as hacking or malicious software (viruses, worms, Trojans). It also covers traditional crimes facilitated by technology, such as fraud, illicit drug trafficking, child sexual exploitation, terrorism and money laundering. High tech methods may be used in such crimes for planning, targeting, coordination, financing, communication or logistics.

The concept of a national centre to coordinate the efforts of Australian law enforcement in combating serious crime involving complex technology was identified as a priority by the Australian Police Commissioners Conference in March 2001. The Australian High Tech Crime Centre was officially launched in July 2003.

The Centre is hosted by the Australian Federal Police (AFP) in Canberra and includes representation from all Australian State and Territory police forces both in its staff and Board of Management. The core team includes investigators, intelligence officers, technical specialists, policy advisors and support staff.

The role of the AHTCC is to:

- provide a national coordinated approach to combating serious, complex and multi-jurisdictional high tech crimes, especially those beyond the capability of single jurisdictions;
- assist in improving the capacity of all jurisdictions to deal with high tech crime; and,
- support efforts to protect the National Information Infrastructure.

The AHTCC fulfils this role through the following functions, which are modelled on the Electronic Crime Strategy, March 2001:

- coordination of high tech crime matters between Australian law enforcement agencies, Federal Government agencies and international agencies;
- investigation of matters either by the AHTCC or through cooperation or referral to a partner agency;
- intelligence services that contribute to a better understanding of the high tech crime environment for the AHTCC, partner agencies, and the wider community through alerts and advisories;
- liaison with Government agencies, industry groups, businesses and other organisations on high tech crime matters, including technical, investigative, business and policy; and,

- knowledge of high tech crime issues such as preventative measures, best practice investigative tools and techniques, expert advice, training and education.

Relationships with industry and business groups have been a key focus for the unit. In May this year the Joint Banking and Finance Investigation Team was established which ensures a coordinated approach to combat the growing trend of phishing—the criminal act of imitating legitimate companies in emails to entice people to divulge their bank details.

Investigations so far have resulted in charges being laid for crimes including Internet banking scams, child pornography and computer hacking. In recent weeks a national operation called “Auxin”, involving the AHTCC, AFP and all State and Territory police agencies resulted in the arrest of more than 200 people in relation to online child pornography.

For more information:

AFP National Media (Canberra): (02) 6275 7100