High Tech Crime Operations (HTCO)

Submission to the House of Representatives Standing Committee on Communications Inquiry into Cyber Crime and its Impact on Consumers

25 June 2009

a) Nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software such as viruses and Trojans

E-Security Threats and Cyber Crime

Technology enabled crime (TEC)[1] is evolving rapidly world wide. Unlike crimes in the physical world, TEC's tend to be voluminous, borderless, anonymous, fast and often low-risk. They span all crime types and are dynamic, incorporating ever-changing and sophisticated technologies. The rapid update of evasive technologies and the use of computer-mediated communication has enabled criminals to commit crimes in a more covert and sophisticated manner.

The Internet is now the popular platform for communication, recruitment, radicalisation, training, fundraising, planning, coordinating, information gathering and data mining. There are examples of many criminal elements operating in the online environment with traditional criminals exploiting technology. Current orthodoxy suggests TEC is not organised into one or more traditional Organised Crime Groups (OCGs) and broadly identifies cyber criminals in a range of TEC's that are interdependent with complementary functionality.

The proceeds of cyber crime are significant – some suggest as high as USD100 billion per year. While the validity of these claims is uncertain the exponential growth of cybercrime is beyond dispute[2].

The growth is fuelled by:

- an online criminal economy which in many respects replicates the legitimate markets;
- increasing broadband connectivity;
- moves towards the automated production of malicious software (malware); and
- ubiquitous online commercial/financial systems.

The criminal environment comprises of cyber criminals ranging from malicious criminals, identity fraudsters, and insiders (disgruntled or

[1] The terms 'Technology Enabled Crime' and 'Cyber Crime' are used interchangeably throughout this document. They generally refer to criminal activity where a computer or network is the source, tool, target, or place of a crime. These categories are not exclusive and many activities can be characterised as falling in one or more. These terms include traditional crimes, such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used.

[2] One global study reported data theft and breaches from cyber crime may have cost businesses as much as $1 trillion globally in lost intellectual property and expenditures for repairing the damage in 2008 (McFee 2009, "Unsecured economies: Protecting vital information" available at http://www.fbiic.gov/public/2009/jan/McAfee_Report--Unsecured_Economies_Protecting_Vital_Information.pdf

corrupt employees[3]) to Organised Criminal Networks (OCNs), OCNs possess fluid structures and exhibit high levels of coordination, communication and organisation. By contrast, traditional OCGs are characterised by their structured, hierarchical formations and their assignment of specific roles to certain members and who are integrating online crime into larger criminal enterprises. OCNs present the greatest threat in this cyber environment as membership and affiliations are in disparate and remote locations with criminals using the Internet to support existing habits. OCGs and OCNs are already established or based in Europe, Africa, Asia-Pacific and North America, with new groups emerging on a regular basis.

The media has a tendency to attribute online crime to traditional OCGs similar to those operating in the physical world. But the reality is that even when online crime is committed by criminal groups — such as the Russian Business Network — they operate in decentralised networks which draw on resources and skills as required for a particular activity rather than operating as part of a centralised hierarchical structure. The temporary and compartmentalised nature of online criminal networks — in addition to the cover of anonymity afforded to online criminals — magnifies the complexity and difficulty of identifying, tracking, investigating and prosecuting criminals operating in cyber environments.

Today's cyber criminal is motivated almost exclusively by financial gain and the attacks are stealthy, targeted and sophisticated. A black economy has developed where criminal capabilities, techniques and tools can be purchased or hired on a commercial basis. These goods and services extend from malware scripting through to the ability to purchase compromised credit card/identity details and the rental of botnets to undertake tasks such as spamming, denial of service attacks, hosting and malware delivery. In addition to theft and fraud, information communication technology (ICT) is now being used to facilitate 'old' crimes such as illicit drug trafficking, child sexual exploitation and people smuggling.

Major vulnerabilities in the current online environment centre around three key elements:

1. Lack of awareness of threats and human susceptibility to social engineering;
2. The exponential growth in malware; and
3. Problems with web architecture and security which leave sites and systems vulnerable to compromise.

[3] Insider cyber crime can be generalized in four main categories: espionage, theft, sabotage, and personal abuse of the organizational network (see also Nykodym, N., Taylor, R., and Vilela, J. 2005, 'Criminal profiling and insider cyber crime', *Computer Law & Security Report*, vol. 21: 408-414.

These vulnerabilities in turn cut across a range of TEC's including, but not limited to, computer intrusions, Internet banking fraud, Domain Name Server poisoning[4], identity crime and unauthorised modification of data.

Malware provides the entry point for many attacks against home users, business and government – and the growth rate of malware is alarming. Recent results from the Australian Institute of Criminology's Australian Business Assessment of Computer User Security (ABACUS) survey has found that sixty-four percent of ABACUS respondents that experienced one or more computer security incidents reporting experiencing a *virus or other malicious code.*[5]

As long as the financial return remains high, these attacks will continue. The low victimisation alert rate associated with these attacks will ensure the criminals continue to fly below the radar due to the extent of the criminal threat, evidenced by the increasing criminal attacks online. Any security response must have at its core an ability to take proactive action that disrupts and dismantles criminal business models and markets. This will require a significant investment in law enforcement to combat TEC.

The demand for more sophisticated malicious software is being driven by the increasing income from compromising systems. This is in turn is making malware stealthier, more targeted and multi-faceted and driving malware business models and structures that closely resemble legitimate business enterprises. OCNs, particularly out of Eastern Europe, are gaining significantly from the opportunity, but criminals outside of these groups who can provide affiliate and support services are also profiting as are less IT savvy criminals who are profiting from the user-friendly nature of modern malware toolkits.

There is a consolidation of effort among individuals to form OCNs who now deploy sophisticated tools and methods for large-scale financial gain and data exploitation rather than mere notoriety. There are indications of traditional OCGs integrating cyber crime into larger criminal enterprises. The future of this trend will include the merging of cyber criminal groups and their technical expertise with organised crime groups and their business acumen to expand the overall reach of organised crime. For

[4] Domain name servers (DNS) convert web addresses into Internet Protocol addresses and routes the computer user to the correct location. Thirteen root DNS servers cover the entire Internet along with a number of local servers. Once reconfigured, the DNS can send users to any number of websites and seriously compromise the entire Internet system. In the case of Domain Name Server poisoning, the list of addresses in a DNS server are altered so that a legitimate URL address points to an illegitimate Internet Protocol address, the fraudulent web site (Brody, R.G., Mulig, G., and Kimball, V. 2007, 'Phishing, pharming and identity theft', Academy of Accounting and Financial Studies Journal,available at http://findarticles.com/p/articles/mi_hb6182/is_3_11/ai_n29363360/?tag=content;col1

[5] Richards K. 2009. *The Australian Business Assessment of Computer User Security: A national survey,* Research and Public Policy Series no. 102, Australian Institute of Criminology: Canberra.

example, Internet fraud and money laundering, long regarded as the specialty of cyber criminals, have proved to be ideal methods of raising funds for terrorism and moving drug money.

The criminal risk to the National Information Infrastructure (NII) and Critical Infrastructure (CI) from computer intrusion and the spread of malicious code is high – particularly where those elements of the NII control financial transactions or hold sensitive commercial/personal identity information. The risk to all NII sectors from state-sponsored attacks — which may be perpetrated under the guise of a criminal attack — is even higher.

Home users are particularly vulnerable to intrusion and online banking fraud due to lower levels of computer security awareness and education, and the presence of unprotected sensitive personal information (such as financial details) on their machines. The machines of the novice home user present a particularly easy target for recruitment into botnets – and compromised machines continue to be used for attacks against commercial and government networks.

Current assessments suggest online crime will continue to be a rapidly evolving landscape, particularly with the current economic downtown and the greater use of social engineering mechanisms to defraud Australian consumers online. The latest of which is the phishing emails which purport to be from one of the major banks, as well as the Australian Taxation Office calling on people to start thinking about lodging their 2008 tax returns[6].

With reports the Australian unemployment rate will rise, triggering a volatile employment market, this may lead to an increase in consumers opting for and being tempted by online money-making schemes, hence resulting in an increase in mule recruitment.[7]

There are indications of traditional OCGs integrating online crime into larger criminal enterprises. The decentralised nature of online crime offers traditional crime groups the opportunity to compartmentalise their operations and to 'shop around' for the most capable and competitively priced services. This practice offers law enforcement points of vulnerability that can be exploited by providing entry points into traditional crime groups. Key areas where traditional crime groups have started to exploit the online environment include fraud, money laundering, fund raising,

6 The email contains a letter stating that it was from ATO. It informs the receiver that he or she is eligible to receive a tax refund. It then asks the recipient to answer the form attached to the mail, click the PRINT button, and then send it to the head office.

7 McAFee 2009. Virtual Criminology Report: Cybercrime versus cyberlaw. McAFee Inc.

victim identification, extortion and counter-intelligence to examine law enforcement capabilities and tactics.

Impact of Malicious Software (Malware)

The production, sale and distribution of malicious code has become a prolific criminal industry throughout the world. Antivirus vendor Symantec identified that malicious code signatures had increased by 265 percent in 2008[8]. According to Trend Micro threat researchers, more than 50 percent of the top 100 malware of 2008 came from the Internet and were accidentally downloaded by users surfing unknown or malicious Web sites. In 2008, McAfee identified an average of 3,500 pieces of malware each day[9]. Concurrent with these trends is a growing global market for antivirus technologies which is expected to reach US$9.6 billion by 2013 (from US$4 billion in 2005).[10]

Criminals are seeking to generate income from accessing confidential data which can be achieved through utilising malware. Featuring high on the shopping list of criminals are personal identity information, bank account details and credit card numbers. Beyond this are targets such as industrial secrets, intellectual property and any information that may be used for extortion purposes.

Malware supports the commercialisation of cybercrime

The growing malware industry has created online organised crime operations with identifiable business models not unlike those run by syndicates in more traditional crime types. A recent example was the well known (but now offline) operation called '76service.' Built around infection by various versions of the 'Gozi' trojan, '76service' offered a subscriber-based service (hosted by RBN[11]) from which users could access units of freshly stolen information from Gozi-infected systems. The '76service' operation had a strong customer service focus. The service included a range of delivery and packaging options designed to help users more easily manage the volume of stolen data to which they had subscribed.

An equally successful business model has grown up around the exploitation of iFrames (inline frames). iFrames are a feature that enables websites to deliver content from a remote website within a floating frame on a page. For example, iFrames can enable sports scores originating on one website to be streamed onto a frame on another site or page.

---

[8] *Symantec Global Internet Security Threat Report: Trends for 2008 available at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf*

[9] McAfee 2009 Threat Predictions Report available at http://www.mcafee.com/us/local_content/reports/2009_threat_prediction_report.pdf

[10] 'Cyber-crime commercialisation spawning malware epidemic' at <http://www.crn.com.au/Tools/Print.aspx?CIID=85834>

[11] Russian Business Network

Criminals exploit iFrames by inserting instructions within the HTML[12] code that makes up the iFrame. These instructions direct the victim's browser to a server controlled by criminals which contains the malware that infects their system.

A common business model to emerge from iFrames is to offer pay-per-infection rates for iFrame infections. Typically, criminals will setup a website offering HTML iFrame code to potential 'affiliates'. Affiliates then sign up to embed this code into unwitting websites. Whenever victims access the malicious iFrame on these websites it generates payments to affiliates according to the number of infections that occur. Some pay-per-infection iFrame sites offer rates that differ markedly depending on the originating country of the victims. Victims originating from wealthier Western nations are more likely to attract higher payments for affiliates due to the potential income that the owner of the pay-per-infection sites can generate from the infected systems.

The professionalisation and commercialisation of the Malware industry is reflected in the emergence of Malware testing kits such as 'KIMS' and 'Scanlix'. These tools can be used to tell a malware author whether their malicious program/code would be detected by one or more of the large range of available anti-virus products. Antivirus vendor PandaLabs claims that they have detected forums where criminals are working together to advance the development of these testing kits.[13]

The modernisation of malware

As the business of malware expands, malware itself has moved with the times to meet the needs of its customers. There is a growing trend towards developing Malware which infiltrates machines and remains undetected for as long as possible.[14]

Malware written to target one or a small number of organisations is on the increase as is malware written to target specific smaller to medium sized businesses.[15] Attackers wishing to carry out such attacks actively gather intelligence on a target such as their IT infrastructure, business and employees and then design an infiltration plan to maximise their chances of success. The nature of this type of malware is that it may be so specifically targeted a sample may never appear on the desk of any anti-

---

[12] HTML means Hyper Text Markup Language. HTML is the language used to create web pages on the World Wide Web.

[13] Dunn, J. 'Criminals automate security testing' at <http://www.networkworld.com/news/2008/030308-criminals-automate-security.html?fsrc=rss-security>

[14] Krill, P. 'Malware's commercialization driving security challenge' at <http://www.infoworld.com/article/06/06/13/79259_HNmalwarestuff_1.html>

[15] Patrizio, A. 'Want a contract with your key logger?' at <http://www.internetnews.com/bus-news/article.php/3661741>

virus vendor. In the IT industry, such malware has become known as 'designer malware'.[16]

Financial and Identity Fraud

Over the past five years, identity crime has increasingly been acknowledged as an emerging threat to the Australian community and Australia's interests. Identity fraud is increasing due to advances in technology in the financial sectors and the rapid increase of commerce through the internet and 'card not present' transactions. As the Government tightens controls at borders and border security, criminals increasingly need false identities to facilitate their crimes.

Consumers, businesses, and any other account-holding entity are at risk from bank fraud. Individual users whose system(s) are relatively open to penetration remain the most vulnerable targets. Individuals and OCN's are seen to be using increasingly sophisticated techniques, which has increased the threat to online consumers.

Stolen credit card numbers and bank account details can be bought online by any user with limited technical knowledge; this could include non-technical members of OCGs and OCNs. As is the case for botnet control software, tools to configure and control malware for the purposes of committing online fraud are becoming increasingly user-friendly.

b) <u>The Implications of these risks on the wider economy, including the growing economic and security impact of botnets</u>

The risk to the Australian economy, particularly Critical and National Information Infrastructure, from computer intrusion and the spread of malicious code by organised crime is high - particularly where those elements of the NII control financial transactions or hold sensitive commercial/personal identity information data. Similarly the risk to other NII sectors is high and it is likely that state-sponsored attacks may be perpetrated under the guise of a criminal attack. Criminal elements with the proper connections could be hired by foreign governments or terrorist organisations to conduct such attacks. The interoperability of outsourcing and criminal affiliations allows access to the resources, human and technical, required to facilitate TEC is easy to come by.

Botnets

Botnets[17] are currently regarded among law enforcement and IT security specialists as the greatest threat to the security and stability of the

[16] 'The Evolving Threat: Combat training for the new era of malicious code' at <www-304.ibm.com/jct03004c/easyaccess/fileserve?contentid=131594>

Internet. To command and control botnets, criminals have slowly been moving away from the use of Internet Relay Chat (IRC) [18] to Hyper Text Transfer Protocol (HTTP)[19] and peer-to-peer (P2P)[20] techniques.

Botnets are used by criminals in a range of online offences including Distributed Denial of Service attacks (DDoS),[21] spamming,[22] hosting malicious websites, and installing malware.[23] Personal home computers form the majority of infected computers. The potential impact on the national economy from DDoS attacks emanating out of vast botnets can not be under estimated.

Recent figures suggest that the number of compromised PC's in botnets has quadrupled in the last quarter alone and these are capable of flooding the internet with more than 100 billion spam messages per day.[24]

Botnets are increasing switching to phishing, DDoS and website attacks which are capable of causing considerable damage and a growing threat to the NII and CI. Botnet derived DDoS attacks have resulted in the degradation and complete disruption of online services in Australia impacting the critical infrastructure such as the financial sector and small and medium enterprises. Such attacks are inexpensive, potentially hugely destructive and can be instigated from all most anywhere in the world.

Investigations undertaken by the Australian Federal Police (AFP) have identified DDoS attacks committed by botnets containing more than 100,000 compromised computers across more than 120 countries. The ability of law enforcement to investigate and prosecute individuals behind such attacks is often thwarted by the transnational nature of the Botnet make up and control systems.

Globally, government agencies have been targeted by botnets and have resulted in the degradation of internet services, loss of confidential information and reduction in government revenue. The attacks on Estonia critical and national information infrastructure in 2007 had a significant impact on government services and communication capabilities across the

---

[17] Botnets are large numbers of zombie computers which hackers have brought under their control after the computers have been infected with malicious software.

[18] IRC is a method of real-time communication over the internet, where users connect to central servers and communicate in one or more discussion forums called 'channels.'

[19] HTTP (Hyper Text Transfer Protocol) is the underlying protocol used by the World Wide Web (WWW). It defines the way information is formatted and transmitted on the WWW.

[20] Peer-to-Peer (P2P) is a type of network that differs from traditional client/server architectures. Rather than reporting to and from a central server, each machine in the network has equivalent capabilities and responsibilities as both 'clients' and 'servers' to other machines in the network.

[21] In a DDoS attack on a network, multiple compromised machines are used to target a system with a view to seriously disrupting it.

[22] Spamming refers to bulk unsolicited email.

[23] Malware is short for 'malicious software' which is designed to damage or disrupt a system.

[24] McAFee 2009. Virtual Criminology Report: Cybercrime versus cyberlaw. McAFee Inc.

country. The attack was reportedly undertaken by botnets consisting of as little as 20,000 compromised computers.

c) Level of understanding and awareness of e-security risks within the Australian community

Irrespective of age, cyberspace plays a vital part in the lives of members of the Australian community. In the last couple of years, Australians are now increasingly becoming aware that in order to remain protected online, there needs to be an understanding and awareness of e-security risks, and how to manage these risks.

According to the Australian Bureau of Statistics (ABS) over 5.8 million Australians were exposed to scams in the 12 months prior to the Personal Fraud 2007 survey[25]. Personal fraud as measured by the ABS involved people receiving and viewing or reading an unsolicited invitation, request, notification or offer, designed to obtain their personal information or money or otherwise obtain a financial benefit by deceptive means. Of those who had received a fraudulent invitation or request, 5.7% (or 329,000 people) became victims by responding to the scam by supplying personal information, money or both, or seeking more information. This equated to a victimisation rate of two percent.

In the most recent incident of credit or bank card fraud, more victims of personal fraud (111,900 people or 29%) had their credit or bank card details obtained from them in person, than through internet or telephone based transactions. However, more than half of the victims of credit or bank card fraud (52.8%) indicated their behaviour had not changed as a result of the incident[26].

This is a clear indication more needs to be done in this area to raise the level of understanding and awareness of e-security risks within the Australian community. It indicates the volume and sophistication of threats online make it imperative that multilayered, real-time protection is used by Australian consumers to ensure online safety.

[25] Australian Bureau of Statistics (ABS), 2008. Personal Fraud Survey 2007. catalogue. No. 452 8.0, ABS: Canberra.

[26] Australian Bureau of Statistics (ABS), 2008. Personal Fraud Survey 2007. catalogue. No. 452 8.0, ABS: Canberra.

d) Measures currently employed to mitigate e-security risks faced by Australian consumers

i) Education initiatives

The AFP's relatively new function - High Tech Crime Operations (HTCO) – is innovative within Australian policing as it combines traditional policing methods, with a greater focus on prevention through education and awareness raising. The AFP recognises the importance of education in raising awareness of the risks faced online and how Australians can empower themselves to mitigate those risks.

Through the creation of a dedicated Crime Prevention Team within HTCO, the role of the AFP is to take a multi-faceted approach to preventing cybercrime. This includes engaging in the following activities aimed at raising the awareness of e-security risks to youth, parents, carers and teachers, and senior citizens and members of the general community.

Youth outreach

- Presentations to schools and youths more generally in the ACT and regional NSW (educating teachers and children on cyber safety, e-security, including tips on how to minimise the risks);
- Giving the youth of today a 'voice' through the Today's Youth Forum and the creation of interactive forums such as a private MySpace profile in which youth have a say in cyber-safety and e-security;
- Participation in the International Youth Advisory Congress (IYAC) in London in July 2008, by sponsoring ten Canberra-based youth to attend and join over 150 youth from countries around to world in creating a safe online environment; and
- Sponsorship of an Australian youth to attend and present at the Third World Congress against the Sexual Exploitation of Children and Adolescents, in Brazil in November 2008.

Community outreach

- Participation in events such as National E-Security Awareness Week (NEAW) through the provision of community and school based presentations on cyber safety and e-security. The AFP's focus this year was on raising awareness amongst senior computer users;
- Joint media releases with Industry (Australian Bankers Association) on online shopping (December 2008); and protecting your financial identity (June 2009).

AFP/other government/non-government departments

- Up skilling of AFP investigators to maximise the opportunities presented by technology and ensure currency and awareness of the use of technology to facilitate crime. This includes the redevelopment of Technology Enabled Crime Awareness program (Tier 1) and Tier 2 which aims to bridge the gap between computer forensics and investigators conducting search warrants and seizing electronic data;
- Liaison and provision of training to other government departments, aimed at increasing knowledge of and appropriate response to issues of technology enabled crime;
- Workshop delivery to the Commonwealth Department of Public Prosecutions; and
- Training of Starlight Foundation 'Livewire' moderators on cyber-safety and e-security.

ThinkUKnow

ThinkUKnow is an initiative developed by the United Kingdom (UK) Child Exploitation and Online Protection (CEOP) Centre. It aims to educate children and young people, as well as their parents, carers and teachers about the risks faced online and how to create a safe online experience.

The UK's ThinkUKnow initiative is a comprehensive educational tool which provides advice, specifically tailored to different audiences, on how to maintain safety in cyberspace and how to report abuse through the Virtual Global Taskforce Report Abuse Button. This empowers young people to take control of their online experience and helps parents and teachers assist them in this endeavour.

The AFP in partnership with Microsoft Australia and the Australian Communications and Media Authority (ACMA), commenced the pilot phase of ThinkUKnow in Australia in Term 1 of the 2009 school year.[27]

The ThinkUKnow pilot entailed the delivery of an internet safety and security education PowerPoint presentation to parents, carers and teachers across selected schools in the Australian Capital Territory, New South Wales and Victoria. The presentation was delivered by two trained volunteers from either the AFP or Microsoft Australia at each school.

A total of 46 presentations were delivered during Term One (February to April) 2009. These presentations have resulted in 2,166 parents, carers, and teachers learning more about keeping young people safe online.

[27] The Australian ThinkUKnow website – www.thinkuknow.org.au - went live on 9 February 2009.

The Centre for Educational Development and Academic Methods (CEDAM) at the Australian National University (ANU) evaluated the ThinkUKnow Australia pilot. Evaluation results indicate the pilot ThinkUKnow program was highly successful and extremely positively evaluated by attending parents, carers, and teachers.

As a result of the successful pilot of the ThinkUKnow program, the AFP and Microsoft Australia will be rolling out the program nationally as of Term 1, 2010.

ii) Legislation and regulatory initiatives

Since the early 1990's the Commonwealth has pursued a range of legislative and regulatory initiatives to combat cyber crime and e-security risks.

The Commonwealth has enacted offences for the misuse of computers and telecommunications systems in the *Criminal Code Act 1995* and created specific offence regimes to address the online sexual abuse of children in the *Criminal Code Act 1995* and spam communications in the *Spam Act 2003*.

Commonwealth law enforcement have been given specific powers for the examination and seizure of computers under *Crimes Act 1914* search warrant including the ability to move a computer off-site for examination, compel the provision of passwords and access data held at another premises via the on-site computer. In addition to more traditional investigative methods Commonwealth legislation enables cybercrime investigators to access telecommunication interception under the *Telecommunications (Interception and Access) Act 1979*, surveillance devices under the *Surveillance Devices Act 2004* and controlled operations incorporating undercover operatives under the *Crimes Act 1914*.

The Commonwealth regulates Internet content through the national classification scheme and the *Broadcasting Services Act 1992*. Internet content that is deemed 'prohibited content' can be added to the Designated Notification Service, colloquially known as the black list. In addition, law enforcement may request carriage service providers to block access to sites suspected of being used to commit offences against Australian law under the *Telecommunications Act 1997*.

The Commonwealth legal and regulatory framework is under constant review.

Informing legislation and regulatory initiatives
In 2009, the AFP, Australian Institute of Criminology (AIC) and Sydney University of Technology co-hosted a High Tech Crime Conference. This inaugural event brought together leading academics, government representatives, law enforcement and members of the judiciary to discuss emerging e-security threats. The outcomes of the Conference will enable greater collaboration between these stakeholders in co-designing responses to the emerging e-security threat environment. It identified a range of potential information sharing, technical exchange and research opportunities available throughout the combined communities. Key amongst these opportunities were:

- Understanding technology and its use by specific criminal groups or to support unique crime types (fraud, child exploitation etc.);
- Identifying new or emerging technologies that offer unique opportunities for criminal groups or specific crime types (mobile phones with communications encryption, encrypted USB devices, speech altering applications, online services that provide for anonymity and security etc.);
- Identifying how quickly the uptake of new technologies occurs within criminal organisations;
- Understanding the technical competency of criminals and determining the extent of criminal service industries (through which criminals obtain technically-skilled assistance on an as-needs basis);
- Legislative gaps in current technology related laws;
- Determining the current extent of judicial and legal understanding of technology related laws;
- Establishing or assisting in the delivery of training programs and working groups for legal professionals and the judiciary involved in prosecuting technology enabled crimes; and
- Outcome of prosecutions (foreign and domestic) which have relied on a technology based legal defence.

iii) Cross-portfolio and inter-jurisdictional coordination

The nature of the AFP, and requirements placed upon it, has changed significantly in recent years. The new challenges the AFP faces include technology-enabled crime, particularly as it intersects with terrorism, illicit drug trafficking, human trafficking and sexual servitude, and other transnational crimes in addition to other roles such as peace operations, aviation security and protection. To address the threat from technology-enabled crime, the AFP established the High Tech Crime Operations (HTCO) portfolio new functional stream in March 2008. The HTCO consolidates the AFP's technology-related prevention and investigative functions into a single portfolio.

The AFP's HTCO portfolio engages with industry specialists and domestic and international law enforcement agencies, through the exchange of information and technological advancements and collaborative learning of operational experiences. This engagement is essential to countering a crime type that has emerged in a rapidly expanding online environment.

HTCO is based on an operating model that enables the AFP to combat technology-enabled crime by leveraging its organisation-wide law enforcement capabilities. This model encompasses the integration of the Australian High Tech Crime Centre (AHTCC) into the AFP thereby enhancing the portfolio's capacity to undertake policy advocacy, crime prevention and education, strategic intelligence support and capability development.

The investigation of technology-enabled crime and e-security incidents is a crucial and growing area of focus for the AFP and maintaining a thorough understanding of e-security threats is an increasing necessity. Essential to the combating of e-security risks is effective agency cooperation and partnership-building across Government, the private sector and internationally.

The AFP maintains strong relationships with a variety of external agencies and the private sector in addressing e-security matters. These relationships are strengthened through membership of key forums such as the Banking & Finance Advisory Group, the Financial Crimes Steering Group and the E-Security Policy Advisory Committee. Separate to the relationships, these committees also provide a policy perspective on operational matters.

At the national level, HTCO builds upon the strong industry and law enforcement agency (LEA) relationships which the AHTCC was instrumental in establishing. In particular, HTCO's affiliations with State and Territory Police have remained strong in recent years due to the cross-jurisdictional LEA membership base of the AHTCC. Prior to its migration into the new HTCO portfolio, the AHTCC operated as a nationally-focused body but comprised representation from each State and Territory Police agency. This meant that AHTCC could maximise cross-agency collaboration under a nationally-consistent approach, resulting in an effective model for undertaking investigations and sharing information and expertise.

In terms of Federal Government partnerships, the AFP has strived to build productive working relationships with several key agencies including the Australian Security Intelligence Organisation (ASIO); the Defence Signals Directorate (DSD); the Australian Taxation Office (ATO); the Defence Intelligence Organisation (DIO); Commonwealth, State and Territory

departments of Attorneys-General; Commonwealth, State and Territory Directors of Public Prosecutions; and the Defence Science and Technology Organisation (DSTO). Effective liaison with these agencies is crucial to the efforts of HTCO in investigating, preventing, regulating and monitoring the online environment.

The establishment of the Joint Operating Arrangement between the AFP, DSD and ASIO in 2000 is critical to the protection and response to threats targeting the NII.

In terms of private sector collaboration, HTCO has been effective in engaging peak industry bodies such as the Australian Bankers Association (ABA), Microsoft, Google, AusCERT and academia.

One example is the Joint Banking and Financial Sector Investigation Team (JBFSIT) which was established by the AHTCC in 2004. The JBFSIT is a unique partnership between law enforcement and the financial sector to actively coordinate a national law enforcement response to online banking fraud involving unauthorised access to financial services through the use of internet based functionalities. Since its inception, the JBFSIT has provided the nexus between Australian law enforcement agencies and the financial sector to effectively target and disrupt persons responsible for online financial fraud offences.

The JBFSIT collaborates with the Australian financial sector through the co-location of bank staff within the AFP at its Melbourne and Sydney offices. Collaboration with the financial sector is focused on prevention strategies to mitigate the impact of on-line consumers from phishing and malicious software. The analysis of data contained within the portal enables law enforcement to identify those responsible for online fraud activities. Offenders are usually based offshore and collaboration with international partner agencies via the AFP International Network is fundamental to the successful investigations and subsequent prosecution outcomes.

Domestically, the AFP continually looks to strengthen relationships with other state and Commonwealth LEAs such as the Australian Crime Commission (ACC) and State and Territory Police. Relationships with State and Territory Police are very important and the AFP is committed to maintaining and enhancing these relationships into the future. National collaboration is fast becoming a priority for Australian LEAs with the ultimate objective being to ingrain cross-agency partnerships and information sharing.

iv) International cooperation

The AFP's HTCO has been instrumental in the AFP's international engagement on technology-enabled crime matters. HTCO has initiated several engagement activities with international LEAs and the private sector. In doing this, HTCO has utilised the AFP International Liaison Officer Network and had forged strategic relationships with key LEAs across Europe, North America and Asia.

In 2003, the AFP became a member of the Virtual Global Taskforce (VGT) along with other key international law enforcement agencies (such as the UK Child Exploitation and Online Protection Centre (CEOP), the U.S. Department of Homeland Security, the Royal Canadian Mounted Police, Interpol and the Italian National Police). This group established strong international partnerships in order to fight online child sexual exploitation on a global scale through crime prevention, education and investigation initiatives.

The AFP has been able to leverage off these connections with the international VGT community in combating other crime types including broader technology-enabled crimes – thus making the VGT affiliation a crucial part of the AFP international engagement strategy.

The AFP is part of the International Watch and Warning Network (IWWN) which was established in 2004 to foster international collaboration on addressing cyber-threats, attacks, and vulnerabilities. The IWWN aims to enhance global cyber-situational awareness and incident response capabilities.

In addition, the AFP is a key member of the Anti-Phishing Working Group (APWG), a global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types. This further strengthens the relationship HTCO has with the ABA in combating and preventing online banking fraud through the work of the Joint Banking and Financial Sector Investigations Teams.

The AFP regularly attends and participates in international cybercrime committees including the Botnet Taskforce, CTINS (Cybercrime Technology Information Network Systems) and the Asian regional Conference on High Tech Crime. HTCO members play a key role in the ongoing Strategic Alliance Group and its subset being the Cyber Crime Working Group.

Internet products and services are often structured to enable users to purchase commodities such as server space or websites from providers

based outside their home nation. This creates practical difficulties when evidence is located in different nations under different laws. In order to address this need for cross-agency cooperation between police agencies, the AFP utilises liaison connections and cooperation with international law enforcement partners in pursuit of criminals using offshore facilities.

The AFP provides a gateway for liaison and collaboration with LEAs around the world. In particular, the AFP conducts intelligence sharing, joint operational activities and capacity building initiatives with international LEAs through the AFP International Liaison Officer Network.

The Strategic Alliance Cyber-Crime Working Group was assembled in 2006, and comprises of the combined law enforcement knowledge and expertise of five countries which have joined to fight TEC in a synergistic way by sharing intelligence, tools and best practices. The AFP joins LEAs from Canada, New Zealand, the United Kingdom, and the United States in this group which is an outgrowth of the Strategic Alliance Group.

Some of the group's activities include:

- developing and launching a series of information bulletins on emerging threats and trends;
- exploring an exchange of cyber experts to serve on joint international task forces and to learn each other's investigative techniques first-hand; and
- conducting shared training curriculums and providing targeted training to international cyber professionals.

The AFP's affiliations with key regional bodies such as the Australia New Zealand Policing Advisory Agency (ANZPAA) are also important to its success on an international scale. Apart from the positive networking opportunities this kind of affiliation provides, ANZPAA gives the AFP access to policing policy and strategic advice, research capacity, knowledge management and information sharing services which are similarly afforded to all Police Ministers and Commissioners throughout the Australian Commonwealth, its States and Territories, and New Zealand.

In September 2007 Australia entered into an operational and strategic agreement with Europol. One of the main functions of Europol is to collate and analyse information provided by member states in the attempt to identify any links between countries that may be affected by the same criminal organisations. Approximately 35 European Union countries and third-member states are co-located at Europol Headquarters in The Hague. Given the criminal activities emanating out of Eastern European nations this partnership will continue to provide significant strategic and

operational intelligence to mitigate TEC threats and assist in the prosecution of organised crime groups targeting Australian online consumers.

In March 2008, the AFP participated in an international cyber-terror exercise to test Australia's response capacity to a cyber-terrorist attack. Termed *Cyber Storm II,* this exercise led by the United States Department of Homeland Security, and built upon the first cyber storm exercise held in February 2006 (of which the AFP was an observer). *Cyber Storm II* involved the government and business sectors of Australia, Canada, New Zealand, the United Kingdom and the United States.

The AFP's AHTCC assisted in scenario development for the event, and the AFP participated in the exercise according to existing national security arrangements outlined in the National Counter-Terrorism Plan.

The international exercise involved simulated cyber and physical attacks targeting critical infrastructure, including the water, energy, information technology, communications, banking and finance industries.

The exercise was beneficial in identifying areas in Australia's national security framework that requires further development. The event served to test partnerships with the private sector, other Government agencies and international agencies.

Overall, the AFP continues to undertake and build on these national and international partnerships through HTCO. Maintaining strong links across the government, law enforcement and private sectors is crucial in enabling the AFP to successfully address technology-enabled crime, and threats to the NII and CI.

e) Future initiatives that will further mitigate the e-security risks to Australian internet users

Public Reporting Arrangements

The DSD Information Security Incident Reporting (ISIR) form has been established to collect information on security incidents which affect the security or functionality of Australian Government computer and communication systems. This information allows high-level analysis of information security incidents, with the ultimate aim of improving knowledge both of threats and vulnerabilities to Australian Government information systems and how to protect these systems more effectively. Information derived from ISIR reporting is also used as a basis for threat assessments and security advice. The types of incidents that commonwealth agencies are asked to report include:

- unauthorised intrusion into an IT system (hacking)
- any compromise or corruption of information
- intentional or accidental introduction of viruses to a network
- intentional or accidental disruption to service or damage to or loss of equipment.

ISIR does not support public reporting and only some Australian States and Territories tend to utilise it. While some NII agencies have also utilised ISIR, it is not designed to handle reporting at the organisational or public level.

Public reporting is not standardised and public perceptions would be enhanced were a simple uniform system to be introduced. Thus far, public reporting of e-security threats has been facilitated through State and Territory Police, the AFP, and AusCERT. Many of these reports are lodged online via each agency's respective website. However, cases reported after often low level incidents, and not usually critical enough to warrant AFP intervention.

Currently, action on more complex issues can be initiated through multiple channels including:

- the National Security Hotline
- the NII Hotline
- the Government Incident Response Hotline.

Legislation

The borderless nature of cybercrime and e-security threats create significant challenges for law makers. The national limitation of laws restricts their ability to effectively address e-security threats which may involve the presence of offenders, victims and evidence in foreign jurisdictions. While the AFP has developed strong international networks that increase interoperability and information sharing with foreign agencies the legislative processes underpinning the formal gathering and exchange of evidence with foreign jurisdictions are not entirely suited for the speed and fluid nature of this crime type. Laws in this area, including the *Mutual Assistance in Criminal Matters Act 1987* and *Extradition Act 1988*, are currently under review by Government.

Internationally there have been a number of initiatives designed to address the jurisdictional issues associated with cybercrime. Of significance is the 2001 Council of Europe Convention on Cybercrime which provides a standard framework for investigating and prosecuting crimes involving computers across national borders. Australia has yet to fully implement the convention with the legislative and policy issues associated with such an implementation still under consideration. The submission of the Attorney-General's Department further discusses this issue.

The ongoing review and reform of legislation is a key consideration in the development of a comprehensive e-security framework. Given the expansive nature of e-security threats a broad range of telecommunications and broadcasting related legislation must be considered to ensure current technologies and future developments are addressed. The following Acts require particular focus:

- Relevant offences in the *Criminal Code Act 1995*;
- *SPAM Act 2003*;
- *Privacy Act 1988*;
- *Broadcasting Services Act 1992*; and
- *Telecommunications (Interception and Access) Act 1979*.

Cloud computing

Cloud computing is a term used to describe the provision of common business applications online. The Google email service Gmail is an example of Cloud Computing. It allows users to view their emails through a web browser, whilst the actual information and software processing remains on Google's servers. Cloud Computing raises a range of issues for law enforcement, the most pronounced of which are questions of jurisdiction, investigation and admissibility of evidence. For example, data accessed by an Australian resident from a server hosted overseas may require a Mutual Assistance Request to that foreign jurisdiction. The integrity and admissibility of such data would also depend on the controls and security placed upon it by the third-party vendor. Proving ownership of the data is further complicated by its potential co-mingling with other data and the degree to which it can be effectively segregated from that data.

In June 2009, HTCO hosted the Australian High Tech Crime Conference. Issues of prosecutorial challenge and legislative change were discussed at the forum with the aim of enabling the Australian government to

anticipate the legal challenges required to adapt to emerging technologies such as Cloud Computing.

Training for the legal profession

The constantly changing cybercrime threat necessitates ongoing training of not only law enforcement personnel but the legal profession, and the judiciary in order to enhance their understanding of TEC and the e-security threat.

Discussions are currently underway with AGD to address this issue, and the outcomes of the AHTC conference will serve to facilitate this further.

f) Emerging technologies to combat these risks.

The AFP is predominantly concerned with offences committed against the Commonwealth, particularly attacks against the NII and CII. It is concerned with organised on-line networks using malicious software to compromise computers and computer systems.

These e-security investigations commonly involve a requirement to analyse large amounts of digital information, often from suspects' hard drives and organisation networks. In response to this, HTCO has installed various technologies to allow investigators to conduct their own analysis of digital information, without the traditional reliance on expert analysts in every instance.

Furthermore, HTCO uses a research and development network which will provide a testing ground for new technologies designed to combat e-security threats.