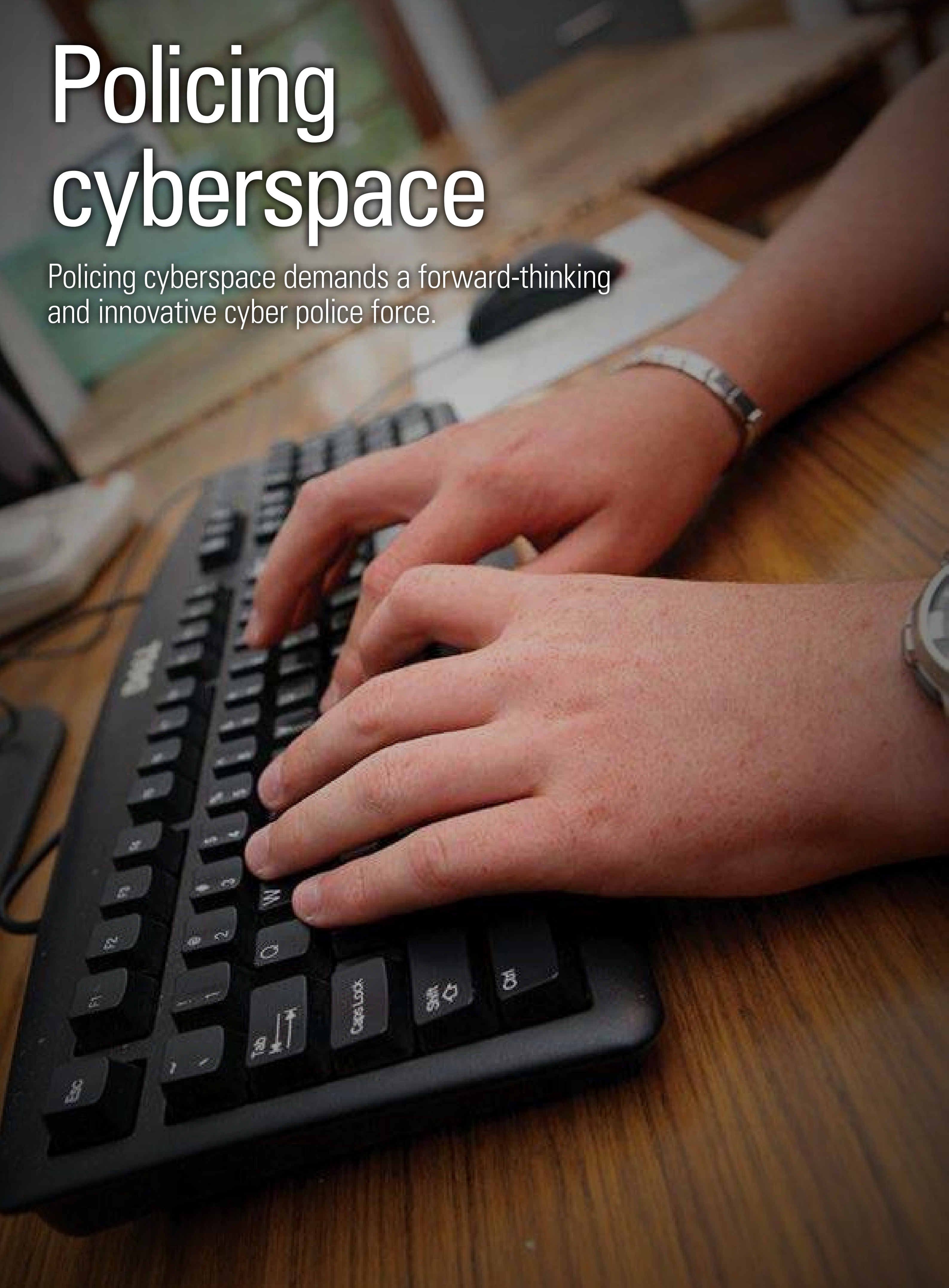
Policing cyberspace

Policing cyberspace demands a forward-thinking and innovative cyber police force.



The investigative arm of the AFP's High Tech Crime Operations (HTCO) portfolio is just that – a focused squad of cyber crime-fighters who operate under the Australian Government's National Security Strategy.

Whether they are catching criminals committing old crimes using new technology or new crimes using the most advanced technology, the two HTCO active arms – Cyber Crime Operations and Child Protection Operations – have one thing in common: a strong focus on bringing to justice those who use technology to commit crime.

"As the primary law enforcement arm of the Commonwealth, it is our job to provide a dynamic response to criminal acts that threaten both the security of Australia's critical infrastructure and information systems that are of national significance," AFP Manager of Cyber Crime Operations, Commander Glen McEwen, explains.

In Australia, the term 'cyber crime' is used to describe crimes that are directed at computers and communications systems, as well as crimes where computers or communications systems are an integral part of an offence.

"Essentially, Cyber Crime Operations investigates significant computer intrusions and collaborates closely with industry and private sector bodies to protect the security and stability of Australia's expanding digital economy," Commander McEwen says.

"We have members operating in Canberra, Sydney and Melbourne but our investigations can take us anywhere in Australia or the world."

He cites Operation Lino, the most significant cyber crime investigation undertaken by Australian law enforcement to date, as a case in point.

"Operation Lino started in Australia with a referral from an Australian bank and grew into a joint international criminal investigation that ended up involving the United States Federal Bureau of Investigation (FBI), the United States Secret Service and the Romanian National Police," he says.

Cyber Crime Operations Team Leader Ashley Wygoda says from as early as October 2010, Romanian cyber criminals had identified a series of vulnerabilities in the point-of-sale computer systems of many Australian retail businesses.

"These vulnerabilities allowed a person with the appropriate skillset to remotely access the computer systems of the Australian retail businesses and discretely remove a variety of files, including those containing customer credit card details," Federal Agent Wygoda says.

Numerous businesses in Western Australia and Tasmania had fallen victim to the syndicate. Thousands of credit card credentials were stolen and neither police service could identify the cause of the problem.

Within a few months of receiving the referral from state jurisdictions, AFP investigators working with the Australian banking and finance sector and industry-based forensic investigators had determined how the credit card details were being stolen.

Federal Agent Wygoda says the perpetrators had identified three separate flaws in the point-of-sale systems of the targeted businesses.

"When combined, these security deficiencies caused clear text credit card information, including a credit card number, expiry date and CVV (card verification value), to be stored on the retailer's computer system without any form of masking or encryption.

"The weak security features in place in each of the affected retailers then allowed the syndicate to access the victim computer systems with relative ease and steal the valuable data, leaving very little evidence of them having done so," he says.

After a lengthy probe to identify the perpetrators, the AFP determined that the syndicate in question was operating out of Romania.

"Through our International Network we sent a detailed intelligence package to the Romanian National Police and commenced a joint investigation with them in March 2012."

The AFP along with the United States Secret Service and Romanian National Police (RNP) were now working on the job. Over the course of 10 months, the

Federal Agent Ashley Wygoda led the AFP's Operation Lino.

RNP identified and targeted the activities of more than a dozen Romania-based cyber criminals involved in the theft of the financial data and production of false credit cards.

"At the same time, our AFP investigators compiled a virtual brief of evidence consisting of statements and computer images from the affected financial institutions and retailers for use in the Romanian criminal courts," Federal Agent Wygoda says.

On 27 November, 2012, more than 200 RNP officers executed 36 search warrants across Romania. More than 150 terabytes of data were seized and 16 people were detained by police. Seven of them were arrested and charged. More than 500,000 Euros, multiple firearms and almost 90 computer servers also were seized. The result was that four "carder" sites – websites that sell stolen credit cards – were dismantled.

An initial assessment of the seized servers indicates the syndicate conservatively had access to over two million stolen credit cards worldwide. This amounts to a potential of about $2.5 billion in fraudulent losses to international banks and financial institutions.

While there are no comprehensive figures available, Commander McEwen says the total cost of cyber crime in Australia could be as high as $4.6 billion annually.

"Cyber crime is a multi-jurisdictional issue, which represents a significant threat to the psychological, social and financial wellbeing of all Australians," Commander McEwen says.

"It affects individuals, businesses and governments alike and is growing in terms of its complexity, level of sophistication and impact. Victims of cyber crime can experience financial losses directly through theft of money, theft of personal information and other data, destruction or deletion of data, fraudulent schemes and extortion."

"However," he adds, "the cyber world is not necessarily financially driven and can also be focused on areas like the interruption or disruption of critical infrastructure systems, the destruction of business enterprises and the sabotage of information systems."

The indirect costs of cyber crime are borne by all and its economic impacts are reflected in a variety of ways, including increased prices and fees to cover business losses, reduced productivity and the funding of measures to respond to the threat.

Tragically, the abuse of the online world and its embedded technologies has also facilitated the ongoing sexual abuse and exploitation of children, who are being abused and then re-abused and victimised

One of the 15 Australian Operation Danton suspects is apprehended.

through internet-facilitated distribution of imagery and the planning of criminal acts.

"The human cost associated with the exploitation of children cannot be quantified in dollar or mental anguish terms, or, for that matter, the ongoing cycle of abuse and recurrent health and social welfare impacts," Commander McEwen says.

It is in the area of travelling child sex offenders, or 'child sex tourism,' and the organised producers of child exploitation material, where the physical and online worlds are inextricably linked. It means that the online elements cannot be attacked in isolation from the underlying physical offending.

AFP National Coordinator Child Protection Operations (CPO), Detective Superintendent Todd Hunter, says the AFP's Operation Danton is a noble example of taking proactive action to counter the crime type.

"In June 2012, Child Protection Operations and the AFP High Tech Crime Operations Internet Policing Team proactively identified and investigated a number of Australians who were sharing and trading child exploitation material using a popular peer-to-peer platform," Detective Superintendent Hunter says.

"Operation Danton involved the identification of the users, covert online engagement and the capture of evidence of their involvement in sharing and trading child exploitation material."

The investigation identified a number of suspects, including 15 Australians. CPO teams executed a number of search warrants resulting in the arrest of 13 men nationwide. Offences related to using a carriage service to access, transmit and possess child exploitation material – offences which carry maximum penalties of 10–15 years' imprisonment.

Storage devices seized during searches contained a significant amount of child exploitation material. These included hard drives, USBs and laptop computers as well as routers. The devices were forensically examined by the AFP Digital Forensic teams and found to contain thousands of child exploitation images.

CPO also identified two children at risk during the operation and ensured through collaboration with the relevant Department of Children's Services that they have been removed from harm and ongoing abuse. A number of charges were also laid in respect of the contact sexual offences against the children identified.

Detective Superintendent Hunter says Operation Danton highlights the strong commitment of CPO to ensuring the safety of children and bringing offenders to account, no matter where they are in the world.

"Operation Danton demonstrates the power of a proactive approach, leveraging the capabilities of

AFP swoops on predators

A referral from German law enforcement of images depicting children, including infants, being sexually abused led to one of the most successful AFP protection operations of 2012.

Operation Belfort led to the arrest of 13 offenders after the AFP was informed of a "quite disturbing" video accessed by Australians on a popular peer-to-peer file sharing network.

The referral from Germany through Interpol identified a number of suspects aged from 21 to 64 across Australia.

AFP Child Protection Operations teams executed 19 search warrants in NSW, Queensland, Victoria and the ACT.

During the execution of warrants, AFP officers seized computers, hard drives, laptop computers, portable storage devices and mobile phones alleged to contain hundreds of thousands of child abuse images and videos.

AFP National Coordinator Child Protection Operations Todd Hunter said Operation Belfort focused on offenders using the peer-to-peer platform.

He said through the use of technology and other methodologies, police could confirm if a person of interest had known child exploitation material.

"We actually have a belief that they have possession of images before we go in the door," Detective Superintendent Hunter said.

"So it's just a matter of confirming and finding the computer they have got it on."

Detective Superintendent Hunter said Operation Belfort was not only successful in bringing 13 offenders to the judicial system but provided further intelligence on offenders and other child exploitation material.

"What we found with a number of those offenders was they had accessed other material over and above the video.

"That allows us to identify other material and identify the victims that are depicted in that material."

Detective Superintendent Hunter said it also allowed law enforcement agencies to further add to the intelligence gathered.

"We pick up other leads on persons that might be dealing or communicating in the online environment," he said.

"We then continue to distribute the intelligence we gather to our partners in the same way that German law enforcement did for us."

An AFP member works on a seized computer during a child sexual exploitation operation.

the AFP's specialist Internet Policing and Digital Forensics teams."

It also shows the benefit of working in partnership with state, territory and international law enforcement agencies, government organisations and industry to combat online child sexual exploitation.

CPO members routinely monitor, investigate and target offenders who travel offshore and commit sexual offences or use the Internet to facilitate the sexual exploitation and abuse of children.

The AFP also works closely with foreign law enforcement agencies to prosecute offenders overseas and can also prosecute offenders under extra-territorial laws in Australia. The AFP continues to work with international partners through the Virtual Global Taskforce (VGT) to share intelligence gained from Operation Danton and to investigate and prosecute further offenders using the file-sharing network.

Underpinning the operational work, High Tech Crime Operations portfolio also has a strong focus on cyber safety and security awareness. The portfolio works across multiple agencies to implement cyber crime prevention strategies aimed at educating and raising awareness of online risks and empowering all online users to protect themselves online.

"Because we are operating in such a complex digital environment where the level, sophistication and expanse of illegal activity are ever-increasing, we need to take a multi-faceted approach to creating a safer operating environment for all consumers," says Coordinator Strategic Initiatives, Dr Jenny Cartwright.

"This means that as well as the standard law enforcement approach of investigation, arrest and charge, we need to focus our energy on disrupting, mitigating and diverting cyber crime, deterring offenders and educating consumers on cyber safety and security awareness."

One of the best demonstrations of this cyber safety approach is ThinkUKnow – a free program directed at parents, carers and teachers at Australian primary and secondary schools that is delivered by trained volunteers from the AFP, Microsoft, ninemsn and Datacom.

"This program illustrates what can be achieved when law enforcement partners work with industry to educate the Australian community on how to protect themselves online," Dr Cartwright says.

Another community awareness project where the AFP has been able to harness the power of technology is the new Australian Police Child ID App. This is a smartphone tool developed in partnership with the United States Federal Bureau of Investigation that is designed to reduce the impact and incidence of missing persons in the Australian community.

As Commander McEwen says, "The challenge, and the portfolio's strength, is to operate in a crime environment that is as broad as it is deep, as complex as it is diverse, and where the only constant is change itself."

AFP calls for new legislation

The AFP is calling for new legislation to counter the emerging problems of data retention in the digital age.

Communications metadata such as the caller and receiver information and the date and time of a call is no longer required by business for billing purposes and in some instances is not being retained by telecommunications companies.

The emergence of Internet-based data communications, such as Skype and other voice-over-the-Internet phone services, is even more problematic as data vanishes almost immediately unless retained.

When the National Broadband Network is finalised, communications data will be exclusively transmitted through the data network.

Assistant Commissioner Gaughan said communications metadata was the building block for criminal investigations across almost all crime types.

"The business requirements for retaining the metadata are significantly diminishing. Therefore, the amount of information we are retrieving back is doing likewise," Assistant Commissioner Gaughan said.

"Seventeen per cent of all checks by Child Protection Operations are coming back from Telcos with no result. What we know from as little as three years ago is that a very small percentage of checks came back with no result."

The Joint Parliamentary Committee on Intelligence and Security is due to hand down a report on the issue and Assistant Commissioner Gaughan is looking to new legislation that reflects the modern communications environment.

"The plan is that Telcos would retain the data for a period of time still yet to be determined – whether that is six months or two years."

"There are still some security and privacy issues to be worked through. We are very cognisant that privacy needs to be at the forefront of the thinking but we believe this is a critical issue for law enforcement."