VICTORIA POLICE

Victoria Police Submission

Commonwealth Parliamentary Joint Committee on Law Enforcement

Inquiry into the capability of law enforcement to respond to cybercrime

VICTORIA POLICE

VICTORIA POLICE

Introduction

Modern technology has seen the advent of new crimes and increased opportunities for criminals to carry out crimes in new ways. Society is also becoming increasingly reliant on technology in all facets of daily life. This reliance coupled with a lack of sufficient cybersecurity is leaving individuals, businesses, governments and critical services vulnerable to serious harm arising from cyber-dependent[1] and cyber-enabled crime.[2]

The COVID-19 pandemic is widely acknowledged as accelerating society's reliance on technology. While technology enabled Victorians to continue to work, learn and connect during the COVID-19 pandemic, it also emboldened criminals to target technologically vulnerable Victorians, and Australians alike, with relative anonymity.

During and since the COVID-19 pandemic, Victoria Police has witnessed increasingly sophisticated and innovative methods to commit cybercrime. Buoyed by proceeds of crime and access to advanced technology, criminals continue to operate in an environment where law enforcement has minimal influence.

Victoria Police is seeing significant growth in individual and organised criminal activity due to the anonymity, relatively low risk, wide reach and high yield cybercrime can offer. Due to its growing pervasiveness, almost all Victoria Police work units are investigating crimes with a technological element. Very often, cybercrime is considered in the context of financial scams, hacking, identity related crimes, bullying and child abuse material. It is also seen in terrorism, serious and organised crime, ideologically and religiously motivated violent extremism and drug trafficking.

This submission addresses the Inquiry's Terms of Reference and provides a description of Victoria Police's experience relevant to responding to cybercrime.[3] The submission provides Victoria-specific examples and seeks to communicate the urgent need for advanced technical capabilities and legislative frameworks to detect, disrupt and prosecute cybercrime.

Victoria Police welcomes this opportunity to provide a submission to the Inquiry.

[1] Cyber-dependent crime is crime directed at computers or other information communications technologies (ICTs). This includes hacking and denial of service attacks which target networked devices such as computers, smart phones, smart watches and tablets. Without digital technology, these offences cannot be committed.

[2] Technology-enabled crime is crime where computers or ICTs are an integral part of an offence. These crimes can occur without technology but when technology is used, it increases the scale, reach and harm of the offence. For example, frauds and scams, identity crime, child abuse, stalking and harassment, family violence and politically and ideologically motivated violence.

[3] In this submission, cybercrime may be used to broadly refer to cyber-dependent crime and cyber-enabled crime. However, cyber-dependent and cyber-enabled terms are not used interchangeably.

VICTORIA POLICE

The role of Victoria Police

Victoria Police serves the Victorian community and upholds the law to promote a safe, secure and orderly society. Victoria Police fulfills this role in line with functions outlined in the *Victoria Police Act 2013* (Vic) (Victoria Police Act):

- preserving the peace
- protecting life and property
- preventing the commission of offences
- detecting and apprehending offenders
- helping those in need of assistance.[4]

Victoria Police is responsible for detecting, apprehending, and disrupting offenders who commit crimes in Victoria or against Victorians. This includes cybercrimes committed against individuals, businesses, the State government and local governments. Our role is to ensure offenders are brought to justice and victims are supported through victim-centric policing and in compliance with the *Victims' Charter Act 2006* (Vic). This extends to all crime types including cybercrime.

Victoria Police is investigating crimes where offenders use technology as a force multiplier. In effect, this means almost all crimes now involve some form of digital evidence. The successful capture, analysis and use of this evidence depends on digital forensic expertise coupled with the right technology.

The Australian Signals Directorate (ASD) *Cyber Threat Report 2022-2023* released in November 2023 highlighted the increasing risk of cybercrime in Australia. An assessment of the national reporting database ReportCyber identified that of the total 94,000 reports made, 26% were made by Victorians.[5] This represents a disproportionately higher reporting rate relative to the total Victorian population.[6] Crimes reported by individuals to ReportCyber commonly involve identity fraud, online banking fraud, online shopping fraud and investment fraud.[7] Crimes reported to ReportCyber include email compromise, business email compromise fraud and online banking fraud.[8] Victoria receives over 2,000 reports a month with a rolling reported 12-month average total loss to victims of almost $400,000,000.[9]

Recent investigations include ransomware attacks on Fire Rescue Victoria, a regional secondary school, and G4S, and cyber-attacks in 2019 on Barwon Health and Cabrini Health. Victoria Police has also undertaken joint investigations including a recent investigation by the Victorian Joint Anti-Child Exploitation Team (JACET) into the creation of an online child exploitation game.[10]

---

[4] *Victoria Police Act 2013* (Vic), ss 8-9 ('Victoria Police Act')

[5] Australian Signals Directorate (2023) ASD Cyber Threat Report 2022-2023. Available <https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023>

[6] Ibid p 25

[7] Ibid p 34

[8] Ibid.

[9] Internal Victoria Police analysis of Victorian ReportCyber reports.

[10] Australian Federal Police, *Man charged following JACET investigation into child exploitation program* (Media Release) 20 August 2023 <https://www.afp.gov.au/news-centre/media-release/man-charged-following-jacet-investigation-child-exploitation-program>

Victoria Police assists national and international partners to identify and apprehend offenders in their respective jurisdictions, apprehend offenders located in Victoria, undertake joint operations and share intelligence information.

Combatting cybercrime is a strategic priority for Victoria Police and we remain unwavering in our commitment to minimising harms to Victorians and Australians alike through our valuable law enforcement partnerships.

Response to terms of reference

Term of Reference 1: Existing law enforcement capabilities in the detection, investigation and prosecution of cybercrime, including both cyber-dependent crimes and cyber-enabled crimes

Detection

In practice, Victoria Police is operating in a reactive rather than proactive capacity with investigations, victim support and prosecutions taking primacy over intelligence functions. Developing intelligence is critical to understanding offence trends, anticipating future victimisation, locating offenders and driving capability building in response to anticipated threats.

Victoria Police notes the National Anti-Scam Centre (NASC) will soon provide law enforcement agencies with centralised intelligence relating to scam trends. While this intelligence will greatly enhance our understanding of scam trends occurring in Victoria, the ability to act on this intelligence will be limited by existing capacity and capability gaps.

Similarly, while existing referrals from ReportCyber[11] provide an opportunity to develop intelligence relating to cybercrime occurring in Victoria and may lead to further crimes being detected, Victoria Police does not currently have capacity to drive these intelligence functions. ReportCyber refers reports to Victoria Police where victims are Victorian. Once referred, Victoria Police triage and investigate as appropriate. Victoria Police may refer a matter to a relevant law enforcement agency if an identified offender resides in another jurisdiction.

Investigations and prosecutions

Victoria Police conducts high level specialist investigations in response to cyber-dependent crime involving complex technology and generalist investigations involving cyber-enabled crime. Victoria Police also has specialist capabilities relating to digital forensic evidence and cryptocurrency.

Although the circumstances, complexity, seriousness and methods used to commit an offence will differ, investigations necessarily follow a standardised investigative methodology. An investigator will need to establish an offence has been committed, identify and locate the offender, gather evidence

[11] ReportCyber is the Australian Government's online Cybercrime reporting tool for Australian individuals, businesses and governments.

to the standard required to support a successful prosecution and support victims in line with the *Victims' Charter Act 2006* (Vic).

Investigations into cyber-enabled theft offences for example, will follow the same methodology as cyber-dependent Denial-of-Service (DoS) attacks. What differs, is the level of digital forensics required to gather evidence. While legislation provides search and seizure powers, the ability to access, secure and produce digital evidence is being challenged by the pace at which technology is evolving and legislation is being implemented.

Digital forensic challenges also exist in relation to non-cybercrime offending where the use of technology is incidental to a crime but of evidentiary significance. Barriers to accessing digital evidence and doing so efficiently, regularly prevents or delays investigations and subsequent prosecutions. Victoria Police is also experiencing increasing difficulties when seeking to introduce digital evidence to support a prosecution.

In 2022-23 Victoria Police received 26,977 online cybercrime reports through ReportCyber.[12] However, this figure likely under-represents actual impact of cybercrime as most victims do not report.

While Victoria Police is rapidly upscaling our response to cybercrime, the increasing level of cybercrime is placing a significant demand on existing resources.

Digital capabilities

Victoria Police utilises digital capabilities to capture and produce electronic evidence from computers and mobile devices. Digital capabilities are undertaken in a forensically sound manner using industry best practice.

Victoria Police has identified the need for increased capabilities to combat current cybercrime trends. For example, the proliferation and migration of data to cloud-based storage providers creates challenges for law enforcement due to search and seizure limitations. Data encryption and the use of Peer-to-Peer (P2P) applications also present challenges to law enforcement. Whilst current legislation enables Victoria Police to search and seize cryptocurrency, there are legislative limitations relating to search and seizure of data from virtual environments (e.g. cloud storage). [13] Issues also arise in relation to access, quarantine and extraction of digital evidence and supporting production before the courts in line with disclosure obligations.[14] Once legislative frameworks are expanded to better enable search

[12] Internal Victoria Police analysis of Victoria ReportCyber reports.

[13] Section 79 of the *Confiscation Act 1997* (Vic) allows a police officer to apply for a search warrant in respect to any tainted or forfeited property that is or may be located on a property within 72 hours. Under section 92A of the Confiscation Act 1997, Victoria Police can execute a search warrant to seize a digital asset and take relevant steps required to gain exclusive control over the asset. Section 465 of the *Crimes Act 1958* (Vic) provides the mechanism to obtain a search warrant based on reasonable grounds that there is or will be within 72 hours, anything connected or suspected to be connected to a crime. Section 465AAAAF of the *Crimes Act 1958* allows a member to access, copy and convert into documentary form data held in or accessible from a computer or data storage device. Whilst data can be copied under a Crimes Act 1958 warrant, it does not have the same effect of seizure under the Confiscation Act 1997.

[14] Disclosure obligations are outlined in the *Criminal Procedure Act 2009* (Vic). Challenges arise, for example, where documents cannot be disclosed due to access issues arising in relation to data storage devices.

and seizure of data, appropriate tools will be required to ensure electronic capture and production is forensically sound.

From a practical perspective, significant advancements in data storage technology mean that individual mobile phones, for example, can now contain up to 1 terabyte of data. This means an increasing amount of data needs to be processed by law enforcement on each device seized as evidence. This increasing burden on law enforcements' digital forensic processing capacity is further exacerbated as multiple pieces of technology will often be seized as evidence in relation to a single crime.

Law enforcement agencies require the capabilities to not only capture and produce this evidence, but also store, review and process extracted material so that it can be tendered as evidence. Victoria Police is processing an increasing number of devices with larger amounts of data, creating a significant capacity burden.

Legislative capabilities

Where legislation does not keep pace with emerging threats, law enforcement agencies are hampered in their ability to respond on behalf of the community.

In addition to key pieces of Victorian legislation outlined below, Victoria Police will rely on Commonwealth legislation including the *Criminal Code Act 1995* (Cth) (Criminal Code Act), *Crimes Act 1914* (Cth) (Crimes Act 1914) and the *Customs Act 1901* (Cth) (Customs Act) when responding to cybercrime. For example, Victoria Police relies on section 3E search warrants under the *Crimes Act 1914.*

Crimes Act 1958 (Vic)

Cyber-enabled crimes are contained through the *Crimes Act 1958* (Vic) (Crimes Act 1958), for example, investigations occur in response to cyber-enabled grooming and child abuse material (CAM) offences, fraud and blackmail offences, stalking, identity crime and money laundering.[15]

In addition to conducting investigations and pursuing prosecutions for general offences where technology is involved, Victoria Police can investigate and prosecute cyber-dependent computer offences including:

- unauthorised access
- modification with intent to cause serious offence
- unauthorised modification of data to cause impairment
- unauthorised impairment of electronic communication
- possession of data with intent to commit serious computer offence
- producing suppling or obtaining data with intent to commit serious computer offence
- unauthorised access to or modification of restricted data
- unauthorised impairment of data held in computer disk, credit card or other device.

[15] *Crimes Act 1958* (Vic) Part 1

- sabotage and threats to sabotage public facilities by causing an unauthorised computer function.[16]

Following recent legislative amendments,[17] general search warrants issued under section 465 of the *Crimes Act 1958* authorise police officers to:

- break open or unlock a receptacle to determine whether it has a thing that can be seized or is hazardous to a person and deal with that thing to seize it or prevent or mitigate a hazard. It also allows a police officer to remove a receptacle to another place for up to seven days for examination[18]
- seek assistance from specialist(s) with skills or technical knowledge necessary to exercise a warrant and bring them onto a warrant premises along with any equipment, vehicle, animal or material reasonably required to exercise the warrant[19]
- secure electronic equipment for 24 hours in a locked room or under guard to prevent it from being destroyed, altered or interfered with and to allow for an expert to be arranged to operate the equipment.[20] A further application can be made to the Magistrates Court to secure electronic equipment for up to seven days if an expert will not arrive at the premises or complete operating the equipment within 24 hours.[21] Further extension applications can be made if required[22]
- access data held in or accessible from a computer or data storage device, make copies and convert it into documentary form[23]
- give directions requiring assistance from a person with knowledge of a computer or computer network.[24] This may include for example, digital currency exchanges.
- require a person with knowledge of a computer or computer network to provide assistance.[25] This may include for example, digital currency exchanges.

Section 80A of the *Crimes Act 1958* allows Victoria Police to treat certain theft offences[26] occurring outside of Victoria as occurring within Victoria if there is a real and substantial link to Victoria. Real and substantial link with Victoria is taken to mean a significant part of the conduct occurred in Victoria

[16] Ibid Part 1, Divisions 3(6) and 3(7)
[17] *Major Crime and Community Safety Legislation Amendment Act 2022* (Vic)
[18] Ibid s 465AAAA
[19] Ibid s 465AAAAB
[20] Ibid s 464AAAAC
[21] *Crimes Act 1958* (Vic)s 464AAAAD
[22] Ibid s 464AAAAE
[23] Ibid s 465AAAF
[24] Ibid s 465AAA
[25] Ibid s 465AA. An application can be made at the time of a s 465 application or after a warrant is executed enabling a police officer to require a person to provide any information or assistance that is reasonable and necessary to allow a police officer to access data held in, or accessible from a computer or data storage device seized from a warrant premises, make a copy of the data and convert it into a document or another form intelligible to a police officer.
[26] Relevant offences are contained within s 81-87 and include: obtain property by deception, obtain a financial advantage by deception, false accounting, falsification of documents, liability of Company officer for certain offences, false Statements by Company Directors, suppression of documents, etc, blackmail such as stalking, child exploitation, fraud, theft etc.

or if the conduct occurred wholly outside of Victoria, there was an intention that substantial harmful effects would arise in Victoria and such affects did arise.[27]

Section 247I of the *Crimes Act 1958* also empowers Victoria Police to investigate computer offences committed outside of Victoria so long as the victim's computer or electronic device was located in Victoria. Section 247I also captures conduct undertaken in Victoria affecting a computer or electronic data device located outside of Victoria. The limitations with this provision are further explained below, in response to challenges and opportunities in existing legislative frameworks.

Confiscation Act 1997 (Vic)

When the *Confiscation Act 1997* (Vic) (Confiscation Act) was first drafted, it did not contemplate digital technology including cryptocurrency and non-fungible tokens. Accordingly, it was designed to facilitate the confiscation of physical objects. Recent amendments to the Confiscation Act provide Victoria Police with greater powers to restrain[28], freeze[29] and forfeit[30] digital assets and compel cryptocurrency platforms to provide information about suspects.[31]

For the purpose of the Confiscation Act, an *account* includes digital wallets, digital profiles or any other facility or arrangement provided by a financial institution for storing, buying, selling or exchanging digital assets or claims to digital assets. [32] *Data held in a computer* includes data entered or copied into the computer, data held in any removable data storage device for the time being in the computer and data held in a data storage device on a computer network the computer is on.[33] A *financial institution*[34] includes the provider of a registrable digital currency exchange service[35] and the Confiscation Act enables the addition of other institutions by way of regulations.

Search warrants executed under section 79 of the Confiscation Act give the power to search a premise for tainted or forfeited property including digital assets or the means of accessing or gaining control of a digital asset. The warrant also includes the power to alter, transfer or perform any other transaction in relation to the asset that may be required to gain exclusive control of the asset.

Updated definitions enable Victoria Police to treat digital assets as physical assets which is a powerful tool when responding to cybercrime. However, these powers are reliant on a section 79 search warrant being issued and cannot be exercised under a general search warrant issued under section 465 of the Crimes Act.

---

[27] *Crimes Act 1958* (Vic) s 80A(2)
[28] *Confiscation Act 1997* (Vic) Parts 2, 4 and 4A
[29] Ibid Part 2A
[30] Ibid Part 3
[31] Ibid s 118B
[32] Ibid s 3
[33] Ibid
[34] Ibid
[35] Within the meaning of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)

Crimes (Controlled Operations) Act 2004 (Vic)

The *Crimes (Controlled Operations) Act 2004* (Vic) (Controlled Operations Act) provides for the authorisation, conduct and monitoring of controlled operations.[36] A controlled operation is conducted for the purposes of obtaining evidence that may lead to the prosecution of a person for an offence; and may involve controlled conduct.[37] Controlled conduct is conduct for which a person (a law enforcement officer or civilian participant) would be criminally responsible if not for protections provided by the Controlled Operations Act against criminal responsibility.[38]

Victoria Police can undertake:

- *cross-border controlled operations* in respect of Victorian offences punishable by a maximum term of imprisonment of three years or more, that will be or are likely to be, conducted in Victoria, the Commonwealth or any state except South Australia and the Northern Territory[39]
- *local major controlled operations* that are or will be conducted wholly in Victoria, in respect of Victorian offences punishable by a maximum term of imprisonment of three years or more[40]
- *local minor controlled operations* that are or will be conducted wholly in Victoria, in respect of Victorian offences punishable by a maximum of three years imprisonment or by a fine.[41]

Controlled operations are used to address a broad range of serious criminal offending and can be conducted for a maximum of seven days or three months depending on the operation category.[42]

The Controlled Operations Act requires the satisfaction of certain requirements for a controlled operation to be authorised[43] including, for example the requirements to:

- state the category of operation
- state the participating jurisdictions
- identify the nature of criminal activity in respect of which the controlled conduct is to be engaged in
- identify suspect identities (to the extent known)
- identify the nature and quantity of any illicit goods involved in the operation
- identify the route through which those goods will pass in the course of the operation.[44]

The nature of controlled operations means the information outlined above may not always be known. This is a barrier to using this critical investigative tool.

[36] *Crimes (Controlled Operations) Act 2004* (Vic) s 1
[37] Ibid s 6
[38] Ibid s 7
[39] Ibid s 9
[40] *Crimes (Controlled Operations) Act 2004* (Vic) s 10
[41] Ibid s 11
[42] Ibid s 19
[43] Ibid Part 2 Division 2
[44] Ibid s 18

VICTORIA POLICE

Crimes (Assumed Identities) Act 2004 (Vic)

The *Crimes* (*Assumed Identities) Act 2004* (Vic) (Assumed Identities Act) enables Victoria Police members, or civilians acting under the supervision of a police member, to acquire and use evidence of an alternative identity for the purpose of facilitating for law enforcement or security purposes, investigations, intelligence gathering (and other related activities including those extending beyond Victoria) or performing functions in accordance with the Victorian Witness Protection Program.[45]

Surveillance Devices Act 1999 (Vic)

The *Surveillance Devices Act 1999* (Vic) (Surveillance Devices Act) regulates the installation, use, maintenance and retrieval of surveillance devices and restricts the communication and publication of information obtained or connected with the surveillance device.[46]

Term of Reference 2: International, federal and jurisdictional coordination law enforcement mechanisms to investigate cybercrimes and share information related to emerging threats

Victoria Police works closely with other federal, state, territory and international agencies in its efforts to respond to cybercrime.

The Chief Commissioner of Victoria Police is a Board member of the Australian Criminal Intelligence Commission (ACIC) along with heads of federal, state and territory law enforcement agencies and key national security, policy and regulatory agencies.

Victoria Police collaborates with the ACIC and others to gather and share intelligence to combat serious and organised crime (SOC) including cybercrime. This includes through relevant special ACIC operations and special ACIC investigations. For example, Victoria Police shares extensive operational policing data with ACIC having been one of the first jurisdictions to adopt the National Criminal Intelligence System (NCIS) which is an information-sharing platform.[47]

Victoria Police is also a member of the Australian Transnational Serious and Organised Crime Committee (ATSOCC) which coordinates transnational law enforcement, and the Serious and Organised Crime Coordination Committee (SOCCC) which coordinates law enforcement at a national level.

Victoria Police sits on various SOCCC working groups, whose remit span across major crime types including cybercrime, drug trafficking, fraud and sexual offences. Membership of these working groups allows for intelligence and information sharing across law enforcement agencies, as well helping to build national capability.

[45] *Witness Protection Act 1991* (Vic)
[46] *Surveillance Devices Act 1999* (Vic)
[47] Australian Criminal Intelligence Committee, Annual Report 2022-23. Available <https://www.acic.gov.au/sites/default/files/2023-10/2022-23_acic_annual_report_web.pdf>

VICTORIA POLICE

SOC groups are leveraging technology including encrypted communication platforms, malware, the darknet and cryptocurrencies to carry out criminal activity, multiplying the reach and impact of harm to Victorians. Noting this and the seriousness of SOC, the ability to respond to all crime types where technology is utilised, including by leveraging our membership of ATSOCC and SOCCC, is of upmost importance for Victoria Police.

Investigating and disrupting cybercrime against Victorians from offshore

When 128 Victorian schools and kindergartens were targeted by hoax bomb and active shooter phone calls, Victoria Police made the crucial breakthrough in the investigation to disrupt a global campaign of over 2,500 threatening calls worldwide. The calls used encrypted communications and faked local phone numbers. They targeted schools, commercial airlines, police stations, hospitals and other businesses resulting in enormous costs and psychological harm, including evacuations of over 40,000 students and staff around Victoria, halt of businesses, and diversion of commercial flights. Victoria Police cybercrime investigators worked closely with our national and international partners to investigate. Using innovative investigative techniques and specialist capabilities, and working with overseas service providers, Victoria Police identified a vendor selling threats-as-a service on the darknet, the services used, call recordings online, and the offender located overseas. Victoria Police provided this evidence to the overseas police cyber unit, resulting in the arrest and successful prosecution of the offender - stopping the calls worldwide.

Victoria Police, Cybercrime Strategy 2022-2027

Victoria Police also works proactively with Australian and New Zealand law enforcement agencies and other key stakeholders as a member of the Helios Joint Management Group, including on joint or cross-border operations. The Helios Joint Management Group is a mechanism for intelligence sharing and joint operations across law enforcement agencies.

Victoria Police holds memoranda of understanding with Commonwealth, state and territory law enforcement agencies enabling information sharing where appropriate. Victoria Police operates a memorandum of understanding (MOU) with the Australian Signals Directorate through the Australian Cyber Security Centre (ACSC) to facilitate information sharing and referrals in respect to reports made to the ReportCyber system.

Victoria Police also has a strong working relationship with the Australian Transaction Reports and Analysis Centre (AUSTRAC) which is supported by a MOU. An AUSTRAC liaison officer is currently seconded to Victoria Police which in addition to strong working relationships across both organisations, provides a valuable conduit to information sharing and collaborative investigations, especially in relation to money mules[48] and cryptocurrency.

[48] A money mule is a person who launders illicit funds on behalf of a third party. A money mule may not be connected to the criminal activity creating the illicit funds. Further information available: < https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling> and <https://www.aic.gov.au/sites/default/files/2020-05/htcb016.pdf>

In addition to federal and jurisdictional partnerships, Victoria Police work with international law enforcement agencies in the United States of America (FBI, Homeland Security Investigations), New Zealand (New Zealand Police and Department of Internal Affairs) and Europe (Interpol, Europol) to share intelligence, assist with investigations and conduct joint enforcement action. Victoria Police works with the AFP to facilitate engagements with other international law enforcement agencies on an ad-hoc basis.

Joint Anti-Child Exploitation Team (JACET)

In October 2014, Victoria Police Taskforce Astraea and AFP Child Protection Operations merged to form the Joint Anti-Child Exploitation Team (JACET) [pronounced jacket], which reflected both the growing international influence of online child exploitation and the prioritised response by law enforcement agencies.

JACET is staffed by Victoria Police and AFP members across investigation, victim identification, online covert engagement and intelligence teams, and is part of the Cybercrime Division, Crime Command.

JACET is involved in a number of duties including:

- Identifying and rescuing vulnerable children from further harm
- Identifying children in image and video files depicting child abuse material
- Targeting recidivist offenders who use the internet to procure or groom children for sexual purposes, through online covert engagement
- Proactively communicating with offenders who use the internet to procure or groom children for sexual purposes, through online covert engagement
- Identifying and monitoring offenders who use peer-to-peer networks to share known child abuse material
- Liaising with international law enforcement agencies and managing interstate and international referrals in conjunction with the AFP Joint Policing Cybercrime Coordination Centre (JPC3).

Australian Federal Police – Joint Policing Cybercrime Coordination Centre (JPC3)

Victoria Police embeds members into the JPC3 to support joint capabilities across state and territory law enforcement, Commonwealth Government agencies and the private sector. The JPC3 is working well to demonstrate an interdisciplinary approach to law enforcement and opportunities for consistent and targeted intelligence gathering, research, and the development of deterrence, prevention and disruption strategies and outcomes.

Victorian Government Cyber Intelligence and Response Service (CIRS)

The CIRS is administered by the Department of Government Services on behalf of the Victorian Government and was established as part of *Victoria's Cyber Strategy 2021*. The service supports Victorian Government organisations to respond to cyber security incidents[49] and coordinates Victoria's response to significant cyber security incidents affecting multiple sectors or communities.

Victoria Police has no formal arrangements with CIRS. However, as part of the overarching Cyber Strategy, the Victorian Government has undertaken to develop a Whole of Victorian Government Cyber Operating Model to improve cyber risk management across the Victorian Public Service. A joint approach will ensure Victoria Police can undertake law enforcement activities in parallel with business and service continuity responses launched by the CIRS.

Term of Reference 3: Coordination efforts across law enforcement, non-government and private sector organisations to respond to the conduct of cybercrimes and risks of cybercrime

Interdisciplinary partnerships, such as those modelled by the Australian Centre to Counter Child Exploitation (ACCCE) demonstrate the benefit of an integrated approach to addressing certain types of offending. Partnerships provide an opportunity to combine specialist skills, capabilities and capacity. Coordinated efforts also support streamlined services and functions while improving operational and cost efficiency through consolidated resources and expertise.

Addressing cybercrime into the future will need a more coordinated effort across law enforcement, non-government and private sector organisations. Many non-government and private sector organisations have specialist capabilities not currently available to law enforcement. Future partnerships with digital currency exchanges (DCE) would also be a valuable tool when addressing cybercrime using cryptocurrencies as DCE can swiftly detect and disrupt suspect transactions.

One key aspect and enabler to ensuring coordination efforts are effective will be finding the intersect where law enforcement, business and service continuity interests can be satisfied. A law enforcement response will often require the virtual environment to be preserved and data to be extracted. These processes take time and can impact business and service continuity which are the main objectives of cybersecurity incident responses.

[49] Cyber security refers to protecting the confidentiality, integrity and availability of computer systems and data as outlined in the Victorian Government Cyber Security Strategy 2021.

VICTORIA POLICE

Term of Reference 4: Emerging cybercrime threats and challenges affecting Australian entities and individuals, including the scale and scope of cybercrimes conducted in Australia or against Australians

As noted earlier in the submission, in 2022-23, approximately 94,000 reports were made to ReportCyber across Australia. Of these, 26% were from Victoria which represents a disproportionately higher rate of cybercrime relative to the population.[50]

Victorian reports to ReportCyber were made in relation to online fraud or scams, identity theft, sextortion, intimate image abuse,[51] online stalking, ransomware, or other crimes involving technology.[52]

On average, there were 68 cybercrime reports made by Victorians to ReportCyber every day.[53]

It is widely acknowledged that the COVID-19 pandemic accelerated society's reliance on technology. While technology enabled Victorians to continue to work, learn and connect during the COVID-19 pandemic, it also emboldened criminals to exploit an increased reliance on technology and lack of cybersecurity to target vulnerable Victorians and Australians alike.

Victoria Police has seen an exponential increase in cyber-enabled crime by individuals and organised criminal groups due to the anonymity, wide reach, and high yield cybercrime provides. As stated earlier in this submission, this means nearly all investigations involve some form of digital evidence.

Below are examples of cybercrime threats and harms arising from the Victorian perspective.

Cybercrime threats

Child sexual exploitation

Victorian child sex offenders use peer-to-peer (P2P) networking, darknet marketplaces and encrypted chat to access and distribute child abuse material (CAM) files.[54] Possession of CAM is strongly linked to the high-risk offenders have or will commit physical sexual abuse offences against Victorian children.[55]

There were 210 child sexual exploitation and CAM referrals from the Australian Centre to Counter Child Exploitation (ACCCE) to JACET in 2022-23.[56] This represents a 9% increase on 2021-22 figures.

---

[50] Australian Signals Directorate (2023) ASD Cyber Threat Report 2022-2023. Available <https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023>

[51] Intimate image abuse is the creation, distribution or threatened distribution of intimate, nude or sexual image or videos without the consent of the person pictured.

[52] Internal Victoria Police analysis of Victoria ReportCyber reports.

[53] Ibid.

[54] P2P filesharing relates to decentralised networks where each computer acts as a server for the others without the need for a central server.

[55] Various studies, including Seto et al (2011) "Contact Sexual Offending by Men with Online Sexual Offenses", Sexual Abuse: A Journal of Research and Treatment 23(1) 124-145; Bourke and Hernandez (2009) "The 'Butner Study' Redux: A Report of the Incidence of Hands-on Child Victimization by Child Pornography Offenders", Journal of Family Violence 24:183-191.

[56] Data from Victoria Police JACET.

Increasing trends include offenders grooming and extorting Victorian children into self-producing CAM and threatening to release the material to the victims' family and friends, unless financial payments are made (sextortion); Victorian offenders targeting hundreds of child victims; and Victorian offenders paying for live streaming of children overseas involved in sexual abuse.

Intelligence sources that globally monitor internet traffic identified that in the month of October over 7.42 million known CAM images were shared across 1684 IP addresses, in Victoria, via P2P networks. This only relates to P2P activity and images that are already known and previously classified as CAM. These statistics do not consider other cyber enabled activity, such as images shared across the darknet and by encrypted chat.

Family violence

Cyber stalking and cyber harassment have become widespread issues in the family violence context. Increasingly, family violence victims report receiving abuse and threats by phone and social media. There are increasing instances of family violence offenders using technology to track, harass and monitor their victims, while also geotagging photographs taken with smartphones. Many family violence stalkers are using tracking devices to survey their victims, including Find my iPhone, social media and spyware, culminating in family violence intervention order breaches.

Another cyber-enabled crime increasingly being seen in the family violence space is Image-based sexual abuse (IBSA) which can include the non-consensual taking, distribution or threats to distribute explicit images or footage of another person. It has devastating and long-lasting impacts on victim-survivors and their families. Threats to commit IBSA is a common means of maintaining coercive control over an individual, both in a family violence setting, and by offenders to discourage their victim-survivors from reporting sexual offending.

Financial scams

In the 2023 year to November, Victoria Police received 124 ransomware reports from Victorian entities where data has also been stolen; surpassing the 118 ransomware incidents the ASD recorded for all of 2022-23.[57]

Individuals are targeted by scams via phone, email, websites, and social media. Online romance and dating scams involve scammers draining the finances of people looking for romantic partners by pretending to be prospective companions. These types of scams exploit emotional vulnerabilities to extract money, gifts, and personal details. Romance baiting occurs where criminals encourage victims

[57] ASD (2023) *ASD Cyber Threat Report 2022-2023*, <https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023>, page 38.

to participate in fake investment opportunities. SIM swap[58] and remote access scams[59] compromise victim's devices providing access to their bank and social media accounts.

Serious and Organised Crime

Organised cybercrime groups work to a model of cybercrime-as-a-service, where less skilled offenders purchase tools and expertise to commit offences. For example, within ransomware syndicates, there are dedicated salaried roles for malware development, testers, marketing, initial access brokers who gain access to systems for resale, extortion negotiations, and money laundering and an organisational structure that mimics modern day legitimate businesses with managers, recruitment, IT systems administrators and support, finances, and payroll. Affiliates then purchase the ransomware and access and deploy it against victims.

Serious and organised crime (SOC) is a substantial and complex threat to the Victorian community and is increasingly cyber-enabled. Over the last 12 months, the SOC environment in Victoria has changed significantly in terms of the escalation in conflict between organised crime syndicates. Encrypted communications (e.g., Threema, Signal and WhatsApp) are used by criminals to communicate in real time to coordinate criminal activity, including, murder, violence, sexual assault, drugs and firearms trafficking, burglaries, fraud, shop theft and arson. SIM swap scams are used in organised crime to fraudulently obtain smart phones, which are shipped offshore for profit.

Harms and costs to the Victorian community

Cybercrime harms include financial losses, physical injuries, digital, psychological, reputational, political, social and societal harms. Each of these can have an ongoing impact on a victim's personal and professional life.[60] Often, an individual is at risk of a cycle of repeat victimisation.

Financial harms

It is estimated that transnational serious and organised crime (TSOC) activity costs Australia $43.7 billion per year, with an additional cost of $16.4 billion for prevention and response.[61] Cyber-

[58] SIM swap occurs when offenders use stolen identity information transfer a phone number to a new SIM (subscriber identity module) with the same provider, often claiming the existing phone is lost or broken. The victim's phone is disconnected and set to emergency (SOS) calls only, as the service is now connected to a device in the possession of the offender. Taking over a victim's phone number gives access to the 2FA (two factor authentication) text messages sent to phones for password resets and to confirm transactions for financial, email and social media accounts linked to the phone number. This facilitates deceptions, identity crime, harassment and computer offences.

[59] Remote access scams involve offenders contacting victims, often via "pop up" virus warnings and trick victims into giving them access to their devices, and without their knowledge to their bank accounts.

[60] Agrafiotis, I. et al (2018) "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate", <https://academic.oup.com/cybersecurity/article-pdf/4/1/tyy006/27126934/tyy006.pdf>.

[61] Smith, R.G. and Hickman, A. (4 April 2022) Estimating the costs of serious and organised crime in Australia, 2020-21. Statistical Report no. 38. Canberra: Australian Institute of Criminology. <https://www.aic.gov.au/sites/default/files/2022-04/sr38_estimating_the_costs_of_serious_and_organised_crime_v2.pdf>

dependent crime committed against individuals is estimated to cost the Australian economy around $3.5 billion annually.[62]

Victorian cybercrime losses reported to Victoria Police via ReportCyber are now almost half a billion dollars per year and increasing annually.[63]

Separately, Victorian reports to Scamwatch totalled $132 million in 2022-23, a 48% increase on losses reported in 2021-22.

Overall, Victorians made 337,208 reports to ReportCyber and Scamwatch, totalling $1.51 billion[64] in financial losses over the last four years (Table 1). Recorded financial losses do not include unreported cybercrime, which is commonly acknowledged to be significant. Reported figures also do not account for the downstream capital and recurring remediation costs to individuals, business, and government, such as lost time spent attempting to recover and prevent further losses, support services, cyber security, or cyber insurance.

Table 1: Victorian losses reported to ReportCyber and Scamwatch[65]

	2019/20	2020/21	2021/22	2022/223	Total	4 year increase
ReportCyber losses	$105,495,672	$179,423,756	$414,357,655	$492,720,407	$1,191,997,490	+367%
ReportCyber reports	16,254	22,048	22,496	26,977	87,775	+66%
Scamwatch losses	$37,803,015	$61,053,053	$89,203,602	$132,219,557	$320,279,227	+250%
Scamwatch reports	37,957	69,661	68,716	73,099	249,433	+93%

Source: ReportCyber and Scamwatch data.

A recent Australian Securities and Investment Commission (ASIC) report into scam prevention, detection, and response by major banks, underscores that it is individuals who bear the brunt of scam losses, as most customer losses are not paid back by banks.[66] Only $21 million of the total $558 million lost to scams last financial year was reimbursed to customers; that is, less than 4% of financial losses were recovered by Australians.

Physical harms

Crimes against the person are increasingly technology-enabled. In particular, Victorian children suffer abuse from child sexual exploitation involved in the manufacture of CAM and endure lifelong trauma because of it.

---

[62] Teunissen C, Voce I & Smith R, 2021. Estimating the cost of pure cybercrime to Australian individuals. Statistical Bulletin no. 34. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78269

[63] In 2021-22 losses totalled $414,357,655. This increased by 18.9% to $492,720,407 in 2022-23. ReportCyber data of reports referred to Victoria Police.

[64] Total combined losses across ReportCyber and Scamwatch reports.

[65] Internal Victoria Police analysis of ReportCyber and Scamwatch reports.

[66] ASIC (April 2023) *Scam prevention, detection and response by the four major banks*, <https://download.asic.gov.au/media/mbhoz0pc/rep761-published-20-april-2023.pdf>, page 2.

Cyber-dependent crime poses risks of physical damage to information and communication technology (ICT) critical infrastructure and hardware, but also to life. In 2019, ransomware disrupted health service providers and hospitals in Gippsland and south-west Victoria, delaying surgeries and other medical services.

Digital harms

Identity theft and compromises to data, including through unauthorised access and leaks, changes and deletion, are commonplace digital harms affecting Victorians.

In 2020, the World Economic Forum identified cyberattacks, together with data fraud or theft, as two of the top 10 global risks facing the world today.[67] Recent attacks illustrate the severity.

The Optus and Medibank Private data breaches impacted over 942,000 Victorians, many of whom continue to turn to Victoria Police for advice and support as they are at risk of identity crime. Operation Guardian[68] has so far linked over 11,000 cybercrime incidents to the Medibank data breach.

Psychological harms

Financial and other harms from cybercrime are often accompanied by serious psychological impacts for individuals including business and government staff. Victims of cybercrime are often confused, embarrassed and ashamed and this often progresses to mental health impacts such as loss of self-confidence, anxiety, depression, and suicidal ideation. The psychological harms from online sexual grooming, child sexual exploitation and child abuse material are often lifelong.

Reputational harms

Victorian victims regularly report they have lost friends, family, jobs, drivers licenses and credit scores. When businesses and government are victims, harms include damaged public perceptions and goodwill, damaged relationships with customers and suppliers, reduced business opportunities and media scrutiny. Victorian victims reported losing business clients due to reputational harms from identity crime.

Social and societal harms

Social and societal harms include negative public perceptions, disruptions to daily lives and impact on services to the community.

In 2022-23, ransomware attacks against the Victorian State Revenue Office, Fire Rescue Victoria, Port Phillip Prison, Melbourne Custody Centre (G4S), and a regional secondary school disrupted key Victorian community services. Data breaches and ransomware attacks pose ongoing future risks to victims including individuals, businesses, and government services.

---

[67] World Economic Forum, 2020, The Global Risks Report, <http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf>

[68] Operation Guardian is a joint operation between the AFP, all State and Territory Police, ACSC, Australian Banking Association, IDCARE and Customer Owned Banking. It was initially launched in response to the Optus data breach and has subsequently expanded to include the Medibank Private data breach and Latitude Services data breach.

Cybercrime and online safety have replaced family violence as a top five community safety concern for Victorians, highlighting the concern about this offending.[69] This increased concern, undermines perceptions of community safety and confidence in the Victorian and broader digital economy.

IDCARE is the national victim support service for cybercrime and identity crime. Table 2 below tells of the personal impacts cybercrime is having on Victorians every day. It is acknowledged that these harms are occurring across Australia on a large scale.

Table 2: Examples of harms experienced by Victorians from cybercrime

Harms	***Incidents and Victim details***
No food, no money and children were removed from her care	Locked out of Centrelink account (F)
Loss of business clients	SIM Swap. Telecommunication company slow to inform them, as a result they were unable to react fast enough to stop further misuse (F, 35-44)
Cancelled holiday because of financial loss	Wallet stolen, bank cards used fraudulently, and funds stolen (M, 25-34)
Business closed from mental health and debt	Multiple misuse of identity events (M, 35-44)
Cost of a new laptop	Access to bank account, IP address compromised (F, 35-44)
Lost driver license and at risk to lose job, as driving is a job requirement	Fraudulent traffic infringements and purchase of vehicles (M, 25-34)
Ruined her business as a massage therapist, as could not keep business open without devices	Several devices accessed maliciously; client factory reset these devices which did not fix the access issues. (F)
House foreclosed and her children were removed from her care	Multiple accounts accessed and financial loss (F)
Child support payments suspended due to false income claimed by offenders in fraudulent tax returns	False income statement submitted to ATO (F, 35-44)
Could not pay rent	Relationship scam, client was sending the scammer money over extended period (F)
Lost all savings, unable to pay rent	Telephone scam impersonating bank. Fraud investigation unable to recover funds (F, 25-34)
Facing homelessness	Rental scam, paid a large deposit, requests for refund met with excuses (M, 25-34)
Severe psychological distress and suicide risk when ATO issued a 14-day deadline for a $135,000 debt	Relationship and investment scam, scammer told client they were able to help her financially through MyGov. (F, 65-74)
Physical injuries, homelessness, and identity crime risk	Physically attacked with large loss of personal information and money.
Had to defer mortgage payment	Investment scam endorsed by “Gina Rinehart”, remote access to device gained with large loss of money (F, 55-64)
Family not talking to him, lost job, large financial loss	Employment and investment scam (M, 45-54)

Source: Case studies provided to Victoria Police by IDCARE victim support agency.

[69] Victoria Police, Community Sentiment Survey 2023 Findings. Available <https://www.police.vic.gov.au/service-delivery-consultation>

Challenges

Technology is constantly changing the way criminals commit crimes against Victorians. It also changes how police and specialists must work to disrupt, prevent, respond to and obtain evidence of criminal activity.

Offenders continuing to exploit technological advancements gives rise to complex challenges for Victoria Police, which include:

- SOC entities operate using infrastructure and business models that rival multi-national corporations.
- Digital evidence being held in many modern devices including smart watches, video doorbells, voice assistants like Siri and Alexa, and vehicles.[70]
- Offenders being able to remotely wipe offending behaviour from smart phones.
- Encryption allowing criminals to communicate covertly.
- Social media and messaging applications being used to target victims.
- P2P and gaming networks allowing offenders to share CAM.
- Artificial intelligence being used to create CAM, voice cloning, deep fake images and video, and to write better malicious software and more convincing lures for deceptions.
- Darknet marketplaces and forums selling illicit drugs, guns, CAM and identity information.
- Cryptocurrencies and blockchain technologies facilitating thefts and money laundering.

Victoria Police considers these challenges above and below are likely shared across law enforcement agencies.

Sophistication of information stealing and sale

Data is a valuable commodity that is stolen and sold with corporation-grade technologies and infrastructure. Technologies used by cyber offenders include malware that extracts saved usernames, passwords, business and personal information held on phones, computers, and browsers; data warehouses for data matching; and automated sales sites with advertising and shopping carts. Data is also being sold as a subscription service.

Ransomware has evolved from encrypting files and demanding payments to unlock them, to stealing victim data and threatening to publish it on data leak sites. It now includes distributed denial of service (DDoS)[71] attacks to encourage victims to pay ransoms through victim payment portals.

Encryption and 'Going Dark'

Encryption plays an important role in protection personal data and privacy. Cybercriminals, SOC groups, terrorists, child sex offenders and other criminals take advantage of encryption technologies

[70] Vehicle data can include location and speed data, phone pairing records, parking camera footage and motion sensor data.
[71] DDoS uses thousands, even hundreds of thousands, of victim computers infected with malware to overwhelm a computer system through repeated volume requests for service, such as website visits.

to hide their offending and communications. The inability of police to execute court orders to access such digital evidence as a result of encryption technologies, known as 'Going Dark', and is one of the biggest challenges facing law enforcement. This affects 'data in motion' such as phone calls, email, and chat and 'at rest' data on devices.

Military grade encryption is increasingly designed into our smart phones, computers, and applications to protect user privacy. High end criminals go further by using dedicated encrypted criminal communications devices (DECCDs) with extra features to evade police detection.[72]

The international Operation IRONSIDE[73] in 2021 used the AN0M app, a trojan horse designed by the United States Federal Bureau of Intelligence (FBI). ANOM provided police with a window into the extent to which SOC offenders coordinate and plan their offending through DECCDs, in this case for drug trafficking, money laundering, plots to kill and firearms distribution. In the wake of the IRONSIDE arrests, organised crime figures have become much more security conscious and suspicious of communications devices and diversify the technologies and how they use them, all of which pose new challenges for Victoria Police.

There is an increasing trend of high-level SOC groups operating in Victoria coordinating violence and illicit drug and tobacco activity via encrypted communications on mobile phones and encrypted applications such as Telegram, Signal, Threema, and WhatsApp while residing offshore. Organised crime groups regularly provide offenders with mobile phones for the sole purpose of providing them with direction, instructions and resources relating to committing acts of violence. This includes locations of where stolen cars and firearms have been stored, for collection and use in associated offending.

Anonymisation and obfuscation technologies

Technologies to hide the identity of users online are standard features of freely available consumer level applications. Spoofing technologies allow sophisticated impersonation of email, phone numbers and online spaces, and allow scammers to pretend to be trusted brand names or people. One in six Australian internet users use virtual private networks (VPNs) to appear to come from different locations; mostly to access content not otherwise available locally, and also to avoid identification. TOR (The Onion Router) is an open-source networking technology that enables anonymous web browsing to protect users' privacy, which spawned darknet marketplaces where illicit commodities can be found and purchased.

Social media

Social media platforms are increasingly used to target and engage potential victims, with fake profiles, disinformation, harassment, CAM, sexual grooming, and scams. Social media poses challenges to investigators and cybercrime intelligence to identify offending online; and to digital forensics to access digital evidence held overseas in the cloud. Social media platforms like Facebook are vulnerable to a process called ad cloaking, where cybercriminals are able to swap out legitimate ads that pass screening

[72] DECCDs are mobile electronic devices specifically designed or equipped to permit secure criminal communications and to defeat law enforcement detection. Common features include secure messaging, replacing voice calls, web browsers and disabling geolocation, multiple profiles, 'panic modes', and timed message destruction to prevent access, and wipe or hide data.
[73] AFP (2021) Special Operation Ironside.

processes at the last second for ads promoting scams. Offenders then entice their victims off-platform into encrypted chats.

Tracking devices

Tracking devices and apps, like Apple air-tags and 'Find my phone', allow stalkers and family violence offenders to track their victims. Tracking devices are also used by SOC groups to track deliveries of illicit drugs and targets of violence, which poses challenges for police surveillance and interception operations.

Cryptocurrencies and blockchains

There are now over 26,000 cryptocurrencies that are or have been actively traded at some point and represent a combined market cap of approximately AUD $2.13 trillion; Bitcoin, Ethereum, Monero and Tether are popular examples. They are especially attractive to offenders, including SOC groups in Victoria, to hide the movement and storage of proceeds of crime and facilitate a range of offending, such as trafficking of drugs and CAM.

In 2022-23, 31.1% of all Victorian ReportCyber reports where there was financial loss involved cryptocurrency, which includes theft of cryptocurrency from Victorians or laundering of their fiat funds stolen through scams into cryptocurrencies.

Seizing cryptocurrencies is not the same as seizing physical digital devices. Accessing and reconstructing cryptocurrency wallets and making the required changes on blockchains to legally secure cryptocurrency under the sole control of police is a highly technical process requiring cutting edge skills and up-to-the-minute knowledge of ever-changing cryptocurrency technologies.

CCTV systems

CCTV evidence depicting crimes and criminals is a vital part of initial action for most investigations, particularly those relating to serious crime, and many investigations are solved through the use of CCTV. Modern CCTV systems are often cloud-based, or data is stored on microchips within devices instead of on hard disk drives, for example, in wireless devices such as doorbell cameras that can store days-worth of data and hold critical digital evidence of crimes committed in the vicinity.

Artificial intelligence

Intimate image abuse now includes images and video that are digitally altered using specialised software, known as deepfake technology. Deepfakes use artificial intelligence software to learn from images and recordings of a person to create extremely realistic but false depictions of them doing or saying things they did not actually do or say. Deepfake scams use fake videos of celebrities to promote phony services on major social media platforms like Facebook, TikTok and YouTube, including famous Australians. Scammers use deepfake programs to mimic celebrities on video calls with potential victims. Faked imagery is now also used for sextortion. AI software available in darknet marketplaces, are used by cybercriminals to write better malware and deceive victims. Cybercriminals are using AI to develop messaging to the community to counter cyber security messaging.

Summary

In the face of mounting threats, harms and technical complexities, building capability in response to these types of cybercrimes is critical. It requires police to have advanced technology and expertise at least

commensurate to those held by criminals involved in these types of offending. In many respects, capability requires modern technology and tools, including legislation, to be designed having regard to the fact that most technology in this space will become obsolete in short time periods.

This is particularly important knowing that criminals can engage in criminal activity without adhering to the same set of rules or having the same financial constraints that law enforcement and other agencies do.

Term of Reference 5: The opportunities and challenges of the existing legislative framework in supporting law enforcement to investigate and act upon instances of cybercrime

Legislative amendments are, and will continue to be, necessary to keep pace with criminal activity. Victoria Police has previously highlighted the difficulties faced by law enforcement agencies in obtaining evidentiary material in matters involving encryption.[74] These concerns have previously been expressed at a Commonwealth level by the Department of Home Affairs, Department of Foreign Affairs and Trade and Attorney-General's Department who have described the malicious use of technology to have '...significantly degraded the capacity of Australian national security and law enforcement agencies to access communications, conduct investigations and prevent crimes...'[75].

Currently, there is no express offence which covers the use of deepfake material for criminal purposes. While existing identity crime offences in the *Crimes Act 1958* (Vic) (Crimes Act) go towards addressing some aspects of identity crime using AI, they are unlikely to be of assistance in many deepfake scenarios —especially where there are cross-jurisdictional factors.

Another example where current legislation does not reflect the borderless impact of cybercrime, is in relation to the operation of section 247I of the *Crimes Act 1958* which addresses computer offences and jurisdiction limits.[76] Unlike Crimes Act fraud and blackmail offences, computer offences do not contain provisions outlining that conduct committed outside of Victoria can be an offence if there is a 'real and substantial link' between the conduct and Victoria. Businesses and individuals are increasingly storing their data in cloud services located outside of Victoria. Currently, under the Crimes Act, if a Victorian individual or business has their cloud-stored data accessed by a person in another state or territory, Victoria Police cannot bring any computer offence charges in relation to this conduct. Effectively, Victorians are left exposed and have no recourse through the criminal justice system.

A compounding issue is the current definition of 'data'. Section 247A of the Crimes Act includes the following data related definitions:

[74] Victoria Police, Parliamentary Joint Committee on Intelligence and Security, Inquiry into Extremist Movements and Radicalism in Australia (Cth), Submission (2021).
[75] Department of Home Affairs, Parliamentary Joint Committee on Intelligence and Security Inquiry into extremist movements and radicalism in Australia (Cth), Submission (2021).
[76] Section 247I requires that a computer or device affected by conduct must be in Victoria or the conduct must be committee in Victoria even if the computer of device was not in Victoria.

- *data* includes information in any form and any program or part of a program[77]
- *data held in a computer* includes data entered or copied into the computer, data held in any removable data storge device for the time being in the computer; and, data held in a data storage device on a computer network of which the computer forms part.[78]
- *restricted data* in relation to the office of unauthorised access to or modification of restricted data means data held in a computer to which access is restricted by an access control system associated with a function of the computer.[79]

These definitions and associated offences do not contemplate circumstances where data is copied, shared or used in ways that harm the original owner without the data owner being permanently deprived of that data.

Another aspect in which updated data definitions would assist is in relation to surveillance devices. Victoria Police currently must obtain a warrant to target "metadata" for an individual based on the broad definition of data. Definitions of "data" or "metadata" that link to specific communication would greatly improve police efficiency without compromising individual privacy. This definition would allow for content specific warrants as opposed to warrants relating to supporting carrier or core computing infrastructure.

Another example is increasing access to consumer level 3D printing machines. Working guns have been produced using 3D printers and digital blueprints that have been accessed online. While 3D printed guns are illegal whether or not they are capable of firing, there are currently no offences to ban access, distribution or publishing of digital blueprints for the 3D printing of guns, leaving Victorians exposed to a cyber-enabled crime with life threatening potential.

Possession of malicious software is also not currently criminalised which means individuals are able to develop and distribute which is essentially a tool to carry out criminal activity.

Similar concerns arise in relation to the practice of doxing. This is where an individual's identification information (address, mobile phone number, work etc) is published online which can cause significant harm, fear and place the victim at risk of further criminal offending. Doxing can also occur in combination with posting CAM or intimate images of adults (image-based abuse). While recent legislative amendments address this kind of offending in relation to stalking offences, section 21A of the Crimes Act requires a course of conduct to have occurred to establish an offence. It does not address the harm caused by a single, one-off incident of doxing and image-based abuse which often leads to continued and repeat victimisation through the sharing this data.

[77] *Crimes Act 1958* (Vic) s 247A
[78] Ibid
[79] Ibid s 247G

VICTORIA POLICE

Term of Reference 6: Prevention and education approaches and strategies to reduce the prevalence of victimisation through cybercrime

In 2022 Victoria Police launched a Neighbourhood Policing Framework which outlines how Victoria Police engages with the community to facilitate stronger ties by being highly visible and by prioritising collaborative partnerships.

Community engagement is a key priority for Victoria Police. This includes supporting community awareness of the risks of cybercrime and through face-to-face, online[80] and in-station communications.

Multimodal communication and awareness campaigns ensure information and key safety messages are accessible to victim cohorts in a way that suits them. For example, Victoria Police has undertaken many face-to-face presentations with senior Victorians who prefer personal interaction when discussing key safety measures and concerns. Victoria Police also conducts face-to-face presentations with younger victim cohorts who are increasingly presenting as victims of cyber-enabled crimes such as sextortion and cyber bullying.

Continually strengthening partnerships with law enforcement, government and non-government partners to ensure prevention and education forms part of the community safety response to cybercrime. Nationally consistent messaging around how to reduce the risk of cybercrime will be key in ensuring Australians can protect themselves against criminal activity.

School engagement

As highlighted in this submission, children and young people are overwhelmingly targeted by cybercriminals. The Victoria Police School Engagement Model acknowledges the benefits and positive impact of engaging with the community through schools.

Youth Resource Officers (YROs) are sworn police officers who focus on engaging with young people and supporting their safety and wellbeing. YROs often work with families, schools, youth services and fellow police officers to promote positive engagement between police and young people and to educate the young people and their communities on safety issues.

YROs attend primary, secondary and tertiary education providers to deliver cyber safety presentations which cover:

- bullying, stalking, respectful behaviours
- sexting, sharing intimate images, sextortion, grooming, sexual assault
- identity theft

[80] Victoria Police publishes information and advice on crime prevention, resources and reporting mechanisms across a number of topics including cybercrime through the 'Your Safety' landing page. Available <https://www.police.vic.gov.au/your-safety>

- scams
- reporting processes.

Since February 2022, Victoria Police members have reached over 77,296 young people across a total of 660 presentations. Victoria Police utilise the ThinkUKnow Australia education program designed by the AFP, Commonwealth Bank of Australia, Datacom and Microsoft Australia when presenting to young people.

Victoria Police recently worked with universities in the wake of a virtual kidnapping scam which took place in Victoria targeting international students. Victoria Police issued warnings to the public and through universities about the risks of this cyber-enabled crime.

Crime Stoppers public knowledge campaigns

An extensive series of cybercrime awareness campaigns have been developed by Victoria Police and Crime Stoppers to educate the community on online safety risks.[81] The series covers a range of topics including remote access scams, social media safety and hacking scams. A series of podcasts were also created in 2020-22.[82]

Term of Reference 7: Other related matters

The timelines for evidence gathering in overseas jurisdictions remains a practical challenge for combatting cybercrime.

The Commonwealth Attorney-General's Mutual Assistance Department is responsible for making requests to foreign countries for assistance in the investigation or prosecution of criminal offences.[83]

Australia's mutual assistance system is governed by the *Mutual Assistance in Criminal Matters Act 1987* (Cth) and provides a mechanism for law enforcement agencies to make requests for information that cannot otherwise be facilitated through Victoria Police liaison units.

Mutual assistance requests are used to gather key evidence; however, these requests are often subject to significant delay.

Conclusion

Cybercrime is a wide-reaching crime type. Victoria Police considers it pertinent to reiterate the need to ensure law enforcement agencies are equipped with the necessary capacity and capabilities to not only keep pace but stay ahead of criminal activity. There is a real risk that without substantial

[81] Crime Stoppers Victoria, Online Safety Series. Available <https://www.crimestoppersvic.com.au/current-focus/onlinesafety/>
[82] Crime Stoppers Victoria, Podcast Series. Available <https://www.crimestoppersvic.com.au/current-focus/crime-stoppers-victoria-podcast-series/>

investment law enforcement agencies will continue to remain in a reactive state when responding to cybercrime.

There are several reasons why increased law enforcement capacity and capabilities for responding to cybercrime are vital for a safer Victoria and Australia. A summary of these reasons is listed below:

1. **Proliferation of cyber threats** – law enforcement agencies must keep pace with offending.
2. **Global nature of cybercrime** – cybercrime transcends borders and requires collaboration and coordination among law enforcement and other agencies, government and industry to combat its impact. Systems must be designed to support and enable this.
3. **High economic impact** – improved capacity and capability will minimise the economic impact, protect critical infrastructure and ensure economic stability.
4. **Increasingly complex attacks** – **the** nature of cybercrime requires advanced tools and expertise to investigate and counter the mounting complexity of these crimes.
5. **Protection of personal data** – law enforcement must be well equipped to investigate and prosecute.
6. **National security concerns** – states and territories have a role to play in mounting a robust law enforcement response to cybercrime.
7. **Deterrence** – strengthening law enforcement capacity and capabilities and imposing maximum disruption and impact will be a deterrence mechanism.
8. **Public trust and confidence** – maintaining public trust in the digital environment is critical. A swift and effective law enforcement response is part of building community trust along with operational cybersecurity responses.
9. **Legislative and regulatory compliance** – as cybercrime evolves legislation and regulations must be updated to reflect this evolution and better enable the law enforcement response.
10. **Protection of critical infrastructure** – critical industries including energy, healthcare and finance rely on interconnected digital systems. Strengthening state and territory law enforcement agencies helps safeguard these critical assets.

Addressing the formidable challenge of cybercrime necessitates a holistic and collaborative approach, transcending the confines of individual law enforcement agencies and fostering a united front. In this collective endeavour, the synergy lies in shared knowledge, joint training initiatives, collaborative technology adoption, mutual skill enhancement, and the seamless exchange of intelligence.

To effectively navigate the complex digital landscape, it is imperative that the tide of capability-building lifts all ships – a concerted effort where the strengths of Commonwealth and state and territory law enforcement agencies are collectively harnessed, without compromising the crucial independence of state and territory police.

Finally, Victoria Police emphasises that innovative, responsive and ground-breaking legislative reforms are necessary at the Commonwealth and state level to meet twenty first century crimes.

Collectively, these efforts will more effectively hold offenders to account and reduce harm for all Australians emanating from cybercrime.

Victoria Police thanks the Committee for the opportunity to make a submission to this important Inquiry and welcomes the opportunity to participate in further consultation.