AFP Submission to the Parliamentary Joint Committee on Law Enforcement

Inquiry into the capability of law enforcement to respond to cybercrime

AFP

afp.gov.au

Contents

Introduction

1. The Australian Federal Police (AFP) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Law Enforcement Inquiry into the capability of law enforcement to respond to cybercrime.
2. The AFP operates in a highly complex and rapidly evolving criminal environment and must remain agile and responsive to the changing demands. This submission draws insights from AFP's operational experience in preventing and combatting cybercrime.
3. Cybercrime causes severe harm to the Australian community with the range of threats diversifying and the prevalence of harm continuing to grow. The AFP recognises that Australia is facing increasing, persistent and pervasive cybercrime threats targeting critical infrastructure, governments, industry and the community.
4. The AFP works to protect the Australian community from the direct and indirect impacts of cybercrime including financial loss, interruption to essential services, risks to public safety, mental health issues, reputational damage, and loss of confidence in the digital economy.
5. As per the 2023 Ministerial Direction, the AFP's key focus is the protection of life, protection of livelihoods and Commonwealth interests.
6. As part of the AFP focus on protecting livelihoods, the AFP is committed to deterring malicious actors from targeting the Australian cyber environment across government, industry and the community and protecting Australians from cybercrime.
7. The AFP ensures efforts are focused on identifying, preventing, disrupting and investigating cybercrime. The AFP remains proactive and continually refines on enhancing capabilities to assist with investigation, disruptions and recruitment of specialist personnel. The AFP is continuously looks at enhancing innovation to acquire the tools necessary to disrupt criminal networks.
8. While law enforcement plays a critical role in combating the threat posed by cybercriminals the problem of cybercrime cannot be addressed by law enforcement alone and it does require a multi-faceted approach.
9. A whole-of-government response is critical to ensure that Australia stays ahead of the continuously evolving threat environment. Collaboration and cooperation from Commonwealth and state and territory agencies, as well as industry and non-government organisations (NGOs) is also critical to combatting cybercrime.
10. We need to put collective effort and emphasis into determining appropriate measures to combat cyber criminals and syndicates, which may include the provision of additional powers to Australian law enforcement.

What is Cybercrime

11. Cybercrime is not victimless crime, these are well thought after, targeted and malicious attacks on members of the community. As law enforcements officers we know that cyber attacks are a global issue and has the impact to disrupt and exploit those who are most vulnerable.
12. Cybercrime is a constantly changing frontier of law enforcement and an important issue for the global community.
13. It is important to recognise that in today's fast-paced digital environment most crime will have some element that is cyber-enabled.

14. As per the Australian Government *National Plan to Combat Cybercrime 2022* Australia defines the term 'cybercrime' to describe both:

    - **Cyber-dependent crimes** directed at computers or other information communications technologies (ICTs) (such as computer intrusions and denial of service attacks). These **crimes did not exist prior to the introduction of computers.**
    - **Cyber-enabled crimes** (such as online fraud, identity crimes and child sexual exploitation and abuse), which can increase in their scale and/or reach through the use of computers, computer networks or other forms of ICTs.[1]

15. Cyber-dependent crimes consist of conduct that only exists in the digital world and involves criminal activities where computer systems or ICT are accessed without authority, attacked or denied the ability to function normally. Examples include crimes relating to the exploitation of victims and their computer systems, such as:

    - Business email compromise
    - Malicious software including remote access trojans, keyloggers, viruses and worms
    - Ransomware extortion
    - Remote access scams
    - Botnets
    - Phishing

16. Cyber-enabled crimes in comparison are traditional crimes committed in new ways. Cyber-enabled crimes are those where use of computers or information technology is incidental to the commission of the offence, such as identity theft, online fraud, trafficking in illicit goods, and online child sexual exploitation.

17. Cybercriminals can range from individuals to criminal networks through to politically motivated actors.

18. The motivations for cybercrime can vary significantly, including financial gain, interpersonal conflict, causing societal disruption, or gaining a competitive edge, through to being ideologically or politically motivated.

19. For the purpose of this submission, we will focus on **cyber-dependent crime** noting that there is often significant overlap with cyber-enabled crime.

The Threat Environment

20. The cybercrime ecosystem is continually evolving, enabling cyber criminals to consistently adapt while maintaining resilience to disruption efforts by law enforcement.

21. According to the World Economic Forum, by 2025, cybercrime will become the world's third largest economy, behind the US and China[2].

[1] Australian Government (2022) *National Plan to Combat Cybercrime 2022*, Australian Government

[2] World Economic Forum (2020) 'The Global Risks Report 2020', *Insight Report 15th Edition*, World Economic Forum

22. Malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, sophistication and impact with more than $33 billion reported as lost as a result of cybercrime in 2020-21[3]; and this is only expected to increase.

23. The threat is widespread with a 2023 report by the Australian Institute of Criminology (AIC) Cybercrime *in Australia 2023* found that 65.5% of Australians have been a victim of cybercrime in their lifetime[4].

The Cybercrime Environment by Numbers

Every 6 minutes a cybercrime report was made to ReportCyber (on average), compared to every 7 minutes 2022-23.

Almost **94,000 cybercrime reports** were received through ReportCyber in 2022-23.

In 2022 the Medibank breach alone affected **14 times more people** than all victims or robbery, unlawful entry with intent and theft, nationwide.

Ransomware notifications by Australian Cyber Security Centre (ACSC) **increased by 7 per cent** from 2021-22, 158 entities compared to 148.

Technology as an Enabler

24. Cybercrime is not a new phenomenon; however, the continuing pace of technological advancement, and the borderless nature of cybercrime, means it is occurring at an increasingly alarming rate.

25. Unconstrained by ethics, cybercriminals are able to quickly pivot the way they work and adopt new technologies to maximise their impact and evade law enforcement.

26. Technological advances mean cybercriminal groups can target thousands of Australians at once from anywhere in the world. Cybercriminals share, buy and sell tools and techniques as well as critical datasets obtained illegally through dark web forums and marketplaces.

27. Cybercrime is also increasingly being professionalised, with skilled criminals performing cybercrime as a service or creating malware packages for purchase by other criminals.

28. The AFP has a well developed understanding of the criminal environment and expects that as technology becomes more sophisticated so too will the criminal networks that utilise it.

[3] Australian Cyber Security Centre (2021) ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021, Australian Signals Directorate, Australian Government

[4] Voce I and Morgan A (2023) 'Cybercrime in Australia 2023', *AIC Statistical Report 43*, Australian Institute of Criminology, Australian Government

29. Criminals will likely continue to capitalise by exploiting technological developments to enable cybercrime, making their activities easier, cheaper, faster, and harder for law enforcement to disrupt. Any gaps in the timespan to identify threats will allow criminals to scale-up in newer areas such as the metaverse and enablers such as AI and data leaks. Identifying the exploitation and enablers as early as possible and mitigating their impacts before becoming entrenched will be an ongoing challenge.

30. Increased use of internet of things (IoT) devices, including via encrypted communications, will change criminal activities and challenge investigations. Criminals, foreign powers, and potential victims/recruits will be highly active online, including in cybercrime, terrorism, issue-motivated groups, drugs, money laundering, fraud, human trafficking, child exploitation, and foreign interference.

A Global Threat of Scale

31. We know Australia's most significant cyber criminals and syndicates are based offshore, are highly resilient and deliberately seek to operate beyond the reach of Australian law enforcement.

32. Global connectivity is allowing criminals and syndicates operating offshore to attack Australia making international cooperation across all societal sectors paramount to responding to such criminals.

33. Australia is facing increasingly persistent and pervasive cybercrime threats targeting critical infrastructure, governments, industry and the community. This is evidenced by major cyber incidents against large corporations over the last year, which has resulted in the compromise of personally identifiable information (PII) belonging to **over half of the Australian population**.

34. Cyber-attacks targeting critical infrastructure, government systems and individuals will continue, with the potential to weaken Australia's economy and threaten the privacy of Australians. Recent high profile incidents, impacting millions of Australians, highlight the magnitude in both size and consequence that this threat poses.

35. The impact of cybercrime continues to affect the feelings of safety and wellbeing of victims, and more broadly causes considerable damage to the confidence of the Australian community in the online environment and digital economy.

36. In addressing the current threat environment, the AFP focuses on prioritising:

    - Malware including ransomware;
    - Exploitation of systems, espionage and large scale data exfiltration;
    - Advanced persistent threats,;
    - High harm, high volume cybercrime impacting the Australian economy including business email compromise and remote access scams; and
    - Cybercrime enablers and the facilitators behind them including infrastructure, initial access brokers, financial services and forums.

37. The Annual *Cyber Threat Report 2022*-23 prepared by Australian Signals Directorate (ASD) highlights the continued deteriorating cyber threat environment faced by Australia, with a cybercrime reported every six minutes, an increase of 23 per cent on the previous financial

year. Calls for advice and assistance also increased by 32 per cent on the previous financial year and the average cost of cybercrime to businesses increased by 14 per cent[5].

38. The report clearly demonstrates every Australian must prioritise cyber security, or risk becoming a victim to online adversaries.

39. The AFP maintains a strong understanding of the threat environment to ensure the AFP is best placed to respond to criminal threats wherever they may occur.

The role of the AFP in the fight against Cybercrime

40. The AFP remains committed to upholding and enforcing Commonwealth criminal law and combatting complex, transnational, serious and organised crime in order to protect Australian lives, livelihoods and Commonwealth interests.

41. The AFP's strategic priorities for cybercrime are:

- Growing our people and capabilities
- High impact Commonwealth cybercrime investigations
- Disruption
- Cybercrime prevention and support
- National coordination of the law enforcement response to cybercrime threats

42. The Australian Government has invested various funding measures into AFP's capability to combat cybercrime, including:

- $89.9 million via Australia's Cyber Security Strategy 2020, which the AFP used to support significant cyber capability uplift including the creation of AFP Cyber Command in January 2022.
- $52.4 million under the *2023-2030 Australian Cyber Security Strategy* over five years from 2023-24 (and $11.1 million per year ongoing) to enhance the AFP's capacity to investigate and disrupt cybercrime.

43. Enhancements to the AFP's capabilities and capacity to counter cybercrime include:

- Establishing additional multidisciplinary investigation teams across Australia.
- Expanding the AFP's presence at the ACSC including the establishment of Target Development and Disruption Teams.
- Creating a dedicated Online Covert Engagement Team for cybercrime.
- Developing the cyber skills and resourcing of the AFP to address cybercrime.
- Deploying six offshore Cybercrime Liaison Officers in the US, South Africa, Serbia, the United Kingdom (UK) and European Union Agency for Law Enforcement Cooperation (Europol).

44. Together with our partners, the AFP is leading the way in the fight against cybercrime, expanding and creating new partnerships, cooperation and coordination mechanisms:

[5] Australian Signals Directorate (2023) *ASD Cyber Threat Report 2022-2023*, Australian Signals Directorate, Australian Government

- We established the JPC3 (Joint Policing Cybercrime Coordination Centre) utilising the powers, experience, investigative and intelligence capabilities of Commonwealth and state and territory police, industry and other partners.
- We are building partnerships with the cyber security community and private industry sectors, with a particular focus on the banking and telecommunications sectors.
- We are coordinating national joint taskforces against Business Email Compromise, Ransomware, Remote Access Scams and identity fraud.
- Alongside the ASD, we established Operation AQUILA, our joint standing operation aimed at the highest priority cyber criminals targeting Australia, through complementary legislative powers, intelligence sharing, prevention, disruption and prosecution.

45. The AFP is innovating and pursuing further opportunities to disrupt cybercrime actors, particularly through our joint operations with the ASD and our collaboration with international law enforcement partners.

46. The AFP is also stepping up its prevention efforts with the establishment of a team within the JPC3, which develops preventative strategies targeting cybercrime offenders and education and awareness raising initiatives to help Australians protect themselves from becoming a victim of cybercrime.

47. The AFP, and state and territory police, have also established **Operation GUARDIAN** through the JPC3 to prevent or minimise harm from the misuse of PII arising from recent major national data breaches, including:

    - Medibank;
    - Optus;
    - MyDeal;
    - Latitude; and
    - Go-Anywhere.

48. Cybercrime investigations are often complex, protracted and resource intensive. The demand on the AFP's resources and capabilities will only intensify as Australia continues to experience increasingly persistent and pervasive cybercrime threats.

49. The AFP is one part of the fight against cybercrime and will continue to work together with our government and state and territory partners, and international counterparts to protect the Australian community from cyber threats.

AFP Capabilities

50. The AFP uses a wide range of capabilities in the fight against cybercrime.

51. The AFP is responsible for the investigation of cyber-dependent crime against the Commonwealth Government, critical infrastructure, systems of national significance or those that impact the whole of the Australian economy.

52. The AFP Cyber Command's mission is to make Australia a hostile environment for cybercriminals.

53. The primary purpose of Cyber Command's operational teams is to investigate serious cybercrimes with the aim of disrupting the activities of cyber criminals and bringing them before the courts for prosecution. The primary offence provisions for cyber-dependent crime

are located under Parts 10.7 and 10.8 of the Commonwealth *Criminal Code Act 1995* (the Criminal Code).

54. The AFP's Cyber Command is primarily responsible for investigating:

- Significant computer intrusions and related offences, including cybercrime impacting major computer systems, large corporations, and the Commonwealth Government.
- Collective large scale breaches undertaken to harvest the personal, business and/or financial data from individual computer systems; home users; and businesses.
- The creation, control and distribution of malicious software (e.g. remote access Trojans, botnets, ransomware).
- Cybercrimes which directly impact critical infrastructure including attacks on financial, utilities, health, food and transportation networks and infrastructure.
- Online criminal trading of sensitive data such as financial, commercial and personal data.

55. These offences undermine and directly impact community, government and institutional confidence in online security, the digital economy and broader societal functions and wellbeing.

56. The broadening criminal use of the cyber ecosystem, including the maturation of the cybercrime business model, enhancements to technical enablers and escalation of cybercrime offending and community expectation evidences the ongoing need for bolstered investment in Australian law enforcement.

AFP Results by Numbers

Between 1 July 2022 and 01 September 2023, AFP charged 28 offenders with **87 offences,** and carried out **59 successful disruption activities**.

Operation DOLOS prevented more than **$10.5 million** being lost to cybercriminals using Business Email Compromise from 1 January 2023 to 31 December 2023.[6]

Detecting and Disrupting Cybercrime

57. Detecting and disrupting cybercrime is one of the many ways the AFP contributes to the fight against cybercrime alongside our law enforcement partners.

58. Detection of cybercrime can occur in a variety of ways, including:

- victim reporting via ReportCyber or direct contact with local police;
- the AFP's vast network of domestic and international law enforcement and trusted industry partners, via their own investigations or their regular monitoring of the dark web and data leak sites used by cybercriminals;
- as a result of a significant cyber security incident; and

[6] This figure is correct as at the 3rd of Jan 2024 and will not capture disruptions and preventions occurring late last year that are yet to be quantified and/or determined to be a disruption.

- internally generated leads resulting from AFP target development efforts or separate AFP investigations.

59. After initial detection of unauthorised access, intrusion or other impacts to computer systems there is significant analysis to determine the origin of the attack.

60. Cyber criminals often are technically competent and resourced, persistent and employ a range of anonymisation and obfuscation techniques to hide their identity, location and activities. Subsequent to detection of cybercrime, identification of the origin and attribution to the responsible criminal/s is critical to disrupting the criminal model and activities.

61. Cybercrime causes significant and serious harm to victims. However, because it generally occurs 'virtually' and there are often no prominently visible physical incidents, the impact of harm is often hard to visualise. The AFP acts to seize evidence, such as devices used to commit cybercrime as well as any criminal proceeds and assets.

Case Study: Operation DOLOS (Taskforce targeting business email compromise)

Business Email Compromise (BEC) continues to pose a significant financial risk to the Australian community with ReportCyber recording approximately $80 million in self-reported BEC losses over the 2022-23 financial year[7]. In January 2020, the AFP established Operation DOLOS, a multiagency AFP-led taskforce targeting BEC. The Taskforce includes state and territory police, Australian Criminal Intelligence Commissioner (ACIC), ACSC, AUSTRAC, and the Australian financial sector.

Since the commencement of Operation DOLOS, the taskforce developed new techniques leading to reduced harm to Australians and enterprises. From 1 January 2023 to 31 December 2023, Operation DOLOS prevented **more than $10.5 million** from being lost from Australian and international victims by disrupting the financial operating model used by criminals. From January 2020 to December 2023 Operation DOLOS has prevented **more than $47 million** being lost to cybercriminals conducting BEC[8].

62. The AFP works to disrupt cybercrime through actions that complicate, prevent or halt criminal activity, resulting in the reduction of the entities' capabilities, its influence and ability to harm or victimise.

63. Disruption activities have a very real impact on the criminal model, in conjunction with the AFP's efforts to investigate crimes already having been committed or during their preparation.

64. Disruption is often the aim and result of deliberate and direct actions and/or efforts by AFP teams, often in conjunction with partners. A disruption activity may involve a number of concerted, evolving strategies. These can include arrest, seizures and convictions as well as other less obvious strategies.

65. Overall, strategies may aim to: remove; restrain; reform and re-direct a criminal entity or criminal activities and the power, influence and status with associates, victims and/or the general community.

66. Disruption can also include a variety of activities authorised by the law enforcement powers created by the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (SLAID Act), such as Data Disruption Warrants, allowing the AFP to modify, add or delete data to frustrate the commission of a serious offence.

[7] Australian Signals Directorate (2023) *ASD Cyber Threat Report 2022-2023*, Australian Signals Directorate, Australian Government

[8] These figures are correct as at the 3rd of Jan 2024 and will not capture disruptions and preventions occurring late last year that are yet to be quantified and/or determined to be a disruption.

67. The AFP provides pre-emptive 'forewarning' type advice to potential victims where indices or attempts to commit a cybercrime are observed. One example of such efforts occurred where the AFP obtained intelligence from an overseas partner that cybercriminals had gained access to a server belonging to an Australian health company. Through collaborative partnerships, the AFP rapidly disseminated relevant information to the company, who were able to decommission the server early. This meant the potential criminal activity, including the potential loss of data, was disrupted before harm could occur.

68. The AFP works with Australian Government agencies on issues surrounding attribution, including consideration of cyber sanctions, noting that the Department of Foreign Affairs and Trade is the lead agency on all sanctions including cyber sanctions. To date, no cyber sanctions have been applied under the *Autonomous Sanctions Regulations 2011*.

69. The AFP, along with other Australian Government agencies, are working with UK and US authorities to amplify any sanctions applied by delivering sanctions against common targets.

Case Study: Operation ZINGER

AFP Operation Zinger is an investigation into Australian alleged offenders purchasing and using compromised Australian devices. Operation Zinger is the AFP's parallel investigation with the US Federal Bureau of Investigation (FBI)'s 'Operation Cookie Monster' into the illicit online marketplace named Genesis Market.

A globally-coordinated resolution occurred in April 2023, involving the takedown of Genesis Market which resulted in over 100 people arrested as a result of over 300 police actions across 17 countries.

In Australia, the JPC3 coordinated the resolution involving 27 search warrants across (and in conjunction with) multiple states and territories, disrupting individuals that we allege were buying stolen personal information via Genesis Market to commit various fraud or cybercrime offences, including against financial institutions and government agencies.

The tireless efforts of our members linked disparate pieces of information together to identify Australian-based users, and shared that intelligence with state and territory police colleagues as part of a coordinated plan to take action.

The exact number of Australian victims remains unknown at this stage – so far the AFP has identified more than 36,000 compromised Australian devices available for sale on Genesis Market, which consists of approximately 2 million sets of credentials, including those containing details from MyGov and Australian financial institutions.

Along with Australia, 17 other countries were also involved in this operation: the US, Netherlands, Spain, France, Finland, Germany, Italy, Poland, Romania, Sweden, Denmark, Canada, Switzerland, the UK, Iceland, New Zealand and Estonia.

Genesis Market was an invite-only marketplace that sold login details, web-browsing cookies and other sensitive information stolen from compromised devices and computers around the world.

Buyers could obtain access to banking and personal information – details that could be used to access government services.

Cybercrime investigations of this scale can take years to resolve, but the AFP is committed to protecting Australians personal information as well as identifying and bringing alleged offenders before the courts.

To date, 12 alleged offenders have been arrested in Australia.

Prosecution

70. The AFP seeks to brief relevant Directors of Public Prosecutions subsequent to charging alleged criminals with cybercrime offences. Charges laid may be contrary to Commonwealth and/or State and Territory criminal laws.

71. The ultimate decision whether a matter progresses to court through public prosecution rests with the relevant Director of Public Prosecutions. Further details on the prosecutorial context to cybercrime can be found in the Commonwealth Director of Public Prosecutions submissions to this inquiry.

Intelligence production and dissemination

72. The AFP produces actionable cybercrime intelligence that has led to a range of domestic and international law enforcement successes, including international taskforces and operational weeks of action, resulting in hundreds of arrests globally.

73. Through the application of intelligence processes, skillsets, professional development, relationships and cybercrime knowledge, AFP Intelligence members develop product that adds value to information and provide insights to decision makers, ranging from investigators to senior officers and members from partner agencies, both domestically and internationally.

74. Members of AFP Intelligence are embedded with AFP Cyber Command multi-disciplinary teams, working closely with investigators and technical officers in the AFP's effort to combat cybercrime.

Activities and actions that complement criminal law enforcement

75. The AFP is distinctly aware that criminal law enforcement is not the only means by which cybercrime can be addressed. It must be complemented by a comprehensive suite of measures and actions that have the effect of reducing the incidence of cybercrime impacting Australians and Australian interests.

76. The 2023-2023 Australian Cyber Security Strategy (the Strategy) was released in November 2022 and outlined the Australian government's strategy to improve cyber security, manage cyber risks and better support citizens and Australian businesses to manage the cyber environment around them. Consistent with the Strategy, the AFP continues to work collaboratively with Commonwealth, state and territory agencies, and industry as well as non-government organisations to strengthen Australia's response to cyber threats.

77. The Strategy is supplemented by the 2023-2023 Australian Cyber Security Action Plan (the Action Plan). Some examples of key actions the AFP is contributing to as part of the Action Plan include:

    - Prevention, mitigation and efforts to secure systems - that aim to mitigate the opportunity for cybercrime victimisation.
    - Enhancement to cyber threat sharing and blocking.
    - Strong governance and appropriate evaluation framework for old and new measures and actions.
    - Ensuring that the regulatory regime is adequate - including a civil law enforcement regime that ensures compliance and appropriate sanctions for non-compliance.
    - Victim support – to assist victims to rebuild their systems and livelihood subsequent to falling victim to cybercrime.

Operational Response to Cybercrime

78. The AFP is innovating and exploring further opportunities to disrupt cybercriminals, particularly through our joint operations with ASD and our collaboration with international law enforcement partners with two recent operations of note being Operation Aquila and Operation Guardian.

Operation AQUILA

79. On 12 November 2022, the Attorney General and Minister for Home Affairs and Cyber Security announced a Joint Standing Operation (Operation Aquila) against cybercriminal syndicates between the AFP and the ASD to investigate, target and disrupt cybercriminal syndicates with a priority on ransomware threat groups.

80. On 22 February 2023, the Joint Standing Operation was formalised via a Memorandum of Understanding (MOU) between AFP/ASD focussed on countering cybercrime. The MOU builds on existing AFP/ASD cooperation.

81. Operation Aquila targets the highest priority cyber criminals targeting Australia. AFP's contribution to the Joint Standing Operation includes criminal investigations, target development and disruption, and engagement with key international partners.

82. Operation Aquila activities involve a broad range of potential actions across intelligence sharing, prevention, disruption and prosecution.

83. Disruption can include a variety of activities including those authorised by the law enforcement powers created by the SLAID Act. This includes Data Disruption Warrants, allowing the AFP to modify, add or delete data to frustrate the commission of a serious offence.

84. Disruption efforts span the following activities:

    - Targeting the highest priority cyber threats impacting Australia.
    - Undertaking criminal investigations and operations relating to major cyber incidents and in-turn identifying proactive opportunities.
    - Focusing on targeting the enablers of the cybercrime ecosystem – infrastructure providers, access brokers, cybercrime forums/marketplaces and financial service providers.
    - Coordinating the national approach (including with the JPC3) and internationally via the Five Eyes Law Enforcement Group (FELEG) Cybercrime Community of Practice and the International Cybercrime Operations Group.

85. The AFP and ASD have separate legal authorities, frameworks and oversight arrangements. However, these are used in a complementary way via Operation Aquila.

86. The Strategic Cybercrime Operations Joint Management Group (SCO JMG) provides strategic oversight and direction to the activities occurring under Operation Aquila.

Operation Guardian

87. Organised cybercriminals and state-sponsored espionage and sabotage cause severe harm to the community. This includes direct and indirect financial loss, interruption to essential services, threats to public safety, mental health issues, reputational damage and loss of confidence in the digital economy.

88. An indirect threat from compromised systems containing PII is criminals subsequently selling or using that information. This data can feed into the broader cybercrime ecosystem and result in further criminality and victimisation.

89. On 28 September 2022, the AFP's JPC3 launched Operation Guardian in response to the Optus data breach.

90. Operation Guardian is a joint operation between the AFP and state and territory police to identify, disrupt, charge and prosecute any person seeking to exploit PII obtained from the data breach.

91. Since it was established, Operation Guardian has extended its remit to the data breaches affecting Medibank, MyDeal, Latitude and GoAnywhere. All breaches have resulted in the exposure of PII of Australians, increasing their risk of financial fraud and identity theft.

92. Operation Guardian is separate from AFP investigations into those responsible for the breaches. It focuses on matching ReportCyber reports of fraud or identity theft with any relevant PII datasets that have been exposed online. ReportCyber is Australia's national online register where members of the public can report a cybercrime incident or vulnerability.

93. Through online monitoring, Operation Guardian collects and shares intelligence with stakeholders and policing agencies, such as the ASD and the ACIC.

94. The AFP can determine if an individual is at heightened risk of financial fraud or identity theft from the sharing of their information online. Once the level of risk is established, we provide relevant information to state and territory police for consideration.

95. On 6 October 2022, Operation Guardian executed a warrant on the home of a 19-year-old NSW-based individual in relation to a crime enabled by the exposure of PII. This person was allegedly responsible for using SMS to try to extort more than 90 customers using stolen Optus data. In November 2022, the individual pleaded guilty to two counts of using a telecommunications network with intent to commit a serious offence. In February 2023, the individual was sentenced to an 18-month Community Correction Order, 100 hours of community service and had a conviction recorded.

96. Under Operation Guardian, we continue to monitor the open internet and dark web to identify the sale or proliferation of PII.

97. The connected nature of the digital world makes cooperation with state and territory policing agencies a critical part of combating cybercrime. We will continue to work closely with other policing agencies to reduce potential harm cybercriminals cause to the community.

98. Cybercriminals rely heavily on anonymity to target their victims and complicate law enforcement efforts. Operation Guardian is a high profile example showing that cyber-based offending is not risk free and that we have the capability and intent to identify and bring offenders before the courts (Enforcement).

99. This investigation and subsequent prosecution served as a disincentive to those considering offending (Prevention) and strengthened the resilience of the Australian public to this type of threat by raising public awareness (Response).

Collaboration and Partnerships

100. The AFP is on the frontline addressing and mitigating cybercrime threats. The AFP achieves this through its close collaboration and relationships with traditional and non-traditional partners.

101. As Australia's national policing agency, the AFP works with domestic and international partners spanning: policing; law enforcement, regulatory, intelligence and security agencies; the private sector; and the community.

102. The AFP leads, participates in and contributes to multiple cybercrime related committees (see **Attachment A**), with both Government, research and private entities, at varying levels to leverage complementary legislative capabilities, technical ability, and specialist knowledge to deliver a cohesive, collective and multi-faceted approach to cybercrime.

103. By adopting a multifaceted approach to fighting cybercrime – including prevention, detection, disruption, investigation and prosecution – these partnerships target serious criminals seeking to do harm to Australians and Australia's interests.

104. While the operational response to cyber incidents is led by the AFP and the ASD, the AFP works together with government, state and territory partners, and international counterparts on incident management responses and the establishment of policies and procedures to protect the Australian community from cyber threats.

105. The AFP continues to develop and maintain strong relationships with private industry including finance, banking and telecommunications entities to better inform the understanding of the cyber ecosystem, to provide prevention messaging, and to disrupt cybercriminal activity.

106. As the ecosystem develops and third party cyber incident response providers become more prevalent, the AFP is identifying opportunities to leverage positive relationships with these entities.

Joint Policing Cybercrime Coordination Centre (JPC3)

107. In March 2022, the JPC3 was launched at its purpose-built facility in the AFP's Eastern Command Headquarters in Sydney.

108. The JPC3 uses the powers, experience, and investigative and intelligence capabilities of all Australian policing jurisdictions, industry and other partners to inflict maximum impact on high volume high harm cybercrime affecting the Australian community.

109. The AFP has formalised most partnerships and MoUs with state and territory police, banking and financial sector representatives, and other key stakeholders.

110. The JPC3:

- Coordinates Australia's policing response to high harm high volume cybercrime to maximise impact on the criminal environment;
- Enhances intelligence sharing and target development across Commonwealth, State and Territory police and Industry;
- Coordinates joint taskforces with police and industry partners to counter priority cybercrime threats;
- Provisions national coordination of capability uplift via cross skilling, joint training and collaborative tool development; and
- Communicates nationally consistent prevention, awareness raising and media activities to industry and the public.

111. Law enforcement is just one element of the response to combatting cybercrime. Public education and awareness campaigns, along with engagement with industry and other regulatory measures is essential.

112. The JPC3 has a prevention capability that works with state and territory police, international law enforcement and industry partners to introduce preventative strategies to disrupt and divert cybercrime offenders and strengthen the Australian community against cybercrime threats through education and awareness initiatives.

113. The AFP has strong industry engagement across cyber security and intelligence sectors and the JPC3 is further contributing to this.

114. To date, the JPC3 includes part time seconded members from several major financial institutions and AUSTRAC, as well as full time seconded members from the ACIC, New South Wales Police Force, Queensland Police, Western Australia Police, Victoria Police and South Australia Police, as well as eSafety and National Anti-Scam Centre (NASC).

115. The JPC3 also has seconded members from international law enforcement agencies.

116. It is this spirit of cooperation and collaboration in recognition of the borderless and multifaceted nature of cybercrime that allows the AFP to continue to lead the way in the fight against cybercrime.

Case Study: Operation WICKHAM

In October 2023, the AFP charged a Chinese national for allegedly using an Australian-based crime syndicate to launder $100 million stolen from victims who invested in a global investment scam. The Melbourne man, 37, is the seventh person charged under Operation Wickham, a joint operation between the AFP and the US Secret Service (USSS).

The AFP executed a search warrant at the man's Sydney and Melbourne homes on Wednesday, 25 October, 2023, and charged him with:

- **One count of recklessly engaging, on two or more occasions, in conduct related to the proceeds of general crime, the value of which being greater than $10 million, contrary to section 400.2B(6) of the *Criminal Code Act 1995* (Cth), and**
- **Providing remittance services while unregistered, contrary to section 74(2) of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).**

The maximum penalty for these offences are 15 and 2 years' imprisonment respectively.

Operation Wickham began in August 2022, when the USSS alerted the AFP-led JPC3 that millions of dollars in allegedly scammed funds were being transferred from the US to an Australian business bank account.

The JPC3-coordinated investigation revealed more than $160 million had allegedly been stolen from victims worldwide. While there were some Australian victims, the majority of people scammed were from the US.

It is alleged that of the $160 million stolen in the scam, more than $100 million was laundered through the Changjiang Currency Exchange or transferred into Australian bank accounts linked to fake Australian businesses, before being moved elsewhere.

It is alleged the bank accounts were controlled by the Long River money-laundering organisation, which the AFP alleges was running the Changjiang Currency Exchange.

The Changjiang Currency Exchange is a prominent, multi-billion-dollar money remitting chain in Australia that is the subject of AFP-led Operation Avarus-Nightwolf.

The AFP will allege that while working at the Changjiang Currency Exchange, the alleged offender had a relationship with an offshore crime syndicate and was directly involved in the procurement of straw directors and dummy account holders for money laundering entities.

He allegedly oversaw the establishment of companies, and their associated bank accounts, in an attempt to circumvent Australia's anti-money laundering laws, particularly those relating to funds transfers.

International Partnerships and Capacity Building

117. The AFP has posted Cyber Liaison Officers with key partners, allowing us to proactively target high value cybercriminals offshore. The AFP is also engaging international partners through the FELEG Cybercrime Community of Practice and the International Cybercrime Operations Group.

118. In order to effectively combat the cybercriminal threat the AFP continues to contribute to the uplift in capability of our global partners with particular assistance given to our Indo-Pacific partners.

119. During 2022–23, we supported activities in the Solomon Islands, Papua New Guinea, Timor-Leste, Tonga, Vanuatu, Samoa and Nauru. The program incorporates Cyber Safety Pasifika (CSP), an AFP-led cyber awareness and education program that aims to increase cyber safety and security awareness across the Pacific region. We assisted Pacific partners to encourage community members to practise safe online behaviour and to finalise more cybercrime investigations. To date, the CSP program has been delivered in 19 Pacific Island countries.

120. A mid-term review of the CSP program found that it remains relevant for the current cybercrime environment. The program successfully navigated the challenges presented during COVID-19 by shifting to a virtual environment. The evaluation also found consensus among stakeholders that a return to in-country engagement was essential, as it facilitates deeper learning and relationship building. Once established, these relationships promote sustainable outcomes as CSP provides a key link for Pacific police members and other organisations.

121. Similar to CSP, Cyber Safety Asia is a prevention-oriented program specifically developed for law enforcement personnel across the South-East Asian region. During 2022–23, we continued to support the Philippines Internet Crimes Against Children Centre, which combats online child sexual exploitation and abuse of children in the Philippines in partnership with the Philippine National Police, the National Bureau of Investigations, the UK National Crime Agency and the International Justice Mission.

Case Study – INTERPOL Operation STORM MAKERS

The AFP is working in collaboration with the International Criminal Police Organization (INTERPOL) which has established Operation STORM MAKERS, a co-ordinated operation targeting cyber-enabled human trafficking for the purpose of forced criminality.

For the past several years, INTERPOL has been closely observing a growing crime phenomenon: large-scale human trafficking where victims are lured through fake job ads to online scam centres and forced to commit cyber-enabled financial crime on an industrial scale.

The scale of the trafficking, and its particular nexus with cyber fraud, have been unprecedented, exploiting specific vulnerabilities of the post-pandemic landscape.

The online scam centres represent a double-edged crime threat, exploiting two sets of victims. On the one side, victims drawn into the human trafficking schemes are subject to forced labour and often extortion through a type of debt bondage, as well as beatings, sexual exploitation, torture, rape and even alleged organ harvesting in some cases.

On the other side, the trafficked workers are used to perpetrate a range of online fraud on a second set of victims, increasingly scattered around the world. The schemes include investment fraud, romance scams and frauds linked to cryptocurrency investing and online gambling.

Prevention and Education

122. The AFP recognises a multi-faceted approach to cybercrime is essential to ensure Australia is a hardened target for cyber criminals and syndicates. Prevention and community education is essential to ensuring individuals, business and government take the necessary steps to avoid becoming a victim of cybercrime.

JPC3 Prevention Measures

123. One capability within the JPC3 construct is prevention. The core mission for JPC3 Prevention is to create a safer and more secure digital Australia through cybercrime prevention, education and awareness. There are three pillars within JPC3 Prevention that achieve this objective.

Building Strong Communities

124. JPC3 Prevention deliver various strategies to strengthen the Australian community against cybercrime threats through education and awareness initiatives.

125. The various prevention strategies and measures of the JPC3 are:

- Collaborate closely with cybercrime investigators to develop up-to-date education and awareness material on emerging cyber threats, with real policing case studies and practical tips on how people can protect themselves cybercrime.
- Deliver timely Cybercrime Alerts to Government, state and territory police and industry partners about new cyber threats, intelligence on how cybercriminals are targeting Australians, operational outcomes, and tips on how people can protect themselves from being victims of cybercrime and the steps they can take if they are a victim.
- Assist in the development of 90-second cybercrime prevention videos made available via the AFP website and YouTube. The videos feature JPC3 investigators giving tips about different cybercrimes affecting Australians, such as ransomware, money muling, remote access scams and business email compromise.
- Work closely with partners to develop and amplify education material during relevant cyber-related campaigns, such as Cyber Security Awareness Month in October, Scams Awareness Week in November and the European Money Mule Action campaign led by Europol.
- The JPC3 Cybercrime Prevention team works closely with the ACSC and the NASC to amplify key messages, provide law enforcement context, and actively participate in working groups to help inform national prevention and education.

Key Partnerships and Networks

126. JPC3 Prevention provide a force multiplier for Australia's response to cybercrime through collaborative stakeholder relationships, including:

- Establishing the National Cybercrime Prevention Network in Australia, to identify cybercrime trends, coordinate messaging and share resources between Australian law enforcement agencies.
- Collaborating with industry to inform and align public and private preventative strategies. It promotes the delivery of consistent messaging to the Australian public about current cybercrimes targeting individuals, businesses, and critical infrastructure, by working

closely with State and Territory Police, Banking and financial institutions, eSafety Commissioner, NASC and the ACSC.

- Partnering and contributing to AIC studies, including a current study that delivers cybercrime prevention messaging, over a six-month period, to more than 1,200 Australians. This study analyses the effectiveness of prevention messaging analysis of metrics relating to the overall reach and engagement with the messaging will inform effective ongoing prevention messaging and campaigns.
- Facilitating cooperation with international law enforcement partners to establish cybercrime prevention best practices and introduce them to Australia, such as piloting a youth offender prevention program, which has been successful in Europe.

Offender Prevention and Diversion

127. JPC3 Prevention has driven innovative solutions to deter, divert and disrupt cybercrime offenders by:

- Becoming a member of the International Cyber Offender Prevention Network and participating in the annual conference designed for law enforcement agencies to share preventative strategies and successes in cybercrime offender prevention.
- Adopting a youth cyber offender prevention program, called re_B00tCMP, from Dutch Police and re-working it for the Australian context. The program, targeting young people aged 12-17 who tend to push the online boundaries, will be piloted in March 2024.
- Developing cyber-specific cease and desist letters and working closely with JPC3 investigators who target low-level cybercrime offenders and issue these warning letters to prevent more serious offending that could lead to criminal charges and life altering consequences.

Cyber-Enabled Crime

128. For cyber-enabled crime, the AFP are seeing technology increasingly being used to facilitate crime in new ways to target new victims.

129. One highly impactful cyber-enabled crime type of note is child exploitation.

130. The AFP notes that the PJCLE have recently released their report on the inquiry into ‘Law enforcement capabilities in relation to child exploitation’ and looks forward to contributing to the whole of government response that is being led by the Attorney-General’s Department.

Combatting Cyber-Enabled crime through the Australian Centre to Counter Child Sexual Exploitation

131. Protecting children from sexual abuse, including online exploitation, is a key priority for the Australian Centre to Counter Child Exploitation (ACCCE) which is part of the AFP.

132. The ACCCE was established by the Australian Government in March 2018 in response to the increasing number and severity of reports of child exploitation received by Australian law enforcement.

133. The ACCCE has driven a collaborative national response to online child sexual exploitation since that time in partnership with Australian Government agencies, private sector

organisations and NGOs, to counter the sexual exploitation of children in Australia and offshore.

134. In driving a national response, the ACCCE specifically focuses on countering the online sexual exploitation of children; this includes a range of criminal conduct and offences such as grooming and the creation and/or circulation of child abuse material (CAM).

135. The borderless crime of online child sexual exploitation is difficult to tackle and means our children can be targeted anywhere and at any time. Reports of online child exploitation to the AFP have more than doubled since the ACCCE was launched.

136. In 2022-23, the ACCCE Child Protection Triage Unit received more than 40,000 reports of online child sexual exploitation, up from 14,285 five years ago, reflecting the scale of this horrific crime.

137. The spike in reports reflects increasing levels of online child sexual abuse identified, alongside greater awareness in the Australian community of the issue and knowing how to report it.

138. Working collaboratively with our operational partners, the ACCCE works to use online evidence to identify the crime scene, its location, the offender and ultimately seeks to remove children from further harm.

Case Study – Operation HUNTSMAN

On 1 December 2022, the ACCCE in partnership with Australian Transaction Reporting Analysis Centre (AUSTRAC) announced the national operational strategy to counter the dramatic increase in online sexual extortion of Australian children. Phase 1 was a financial disruption strategy enacted against hundreds of Australians, to significantly reduce the profit that criminals realise from online child sexual exploitation.

The ACCCE is working with a number of domestic and international partners to identify and stop offshore criminal syndicates profiting from Australian children, with rapid initial action to stop the flow of money from Australian victims ever reaching criminal syndicates.

ACCCE have achieved this by identifying over 800 Australians enabling this crime and working with the financial sector to prevent those Australians from being able to facilitate online crime in the future.

The ultimate goal is to stop sexual extortion of children and remove the ability for anyone to generate profit from the sexual exploitation of children within Australia.

Phase 2 of Operation HUNTSMAN involves taking action against all the domestic and offshore elements involved in facilitating or profiteering from online child sexual exploitation. ACCCE are currently working with international partners to disrupt offshore-organised crime syndicates targeting Australian children.

The nature of this offending is known to have increased risks for self-harm.

The primary driver for AFP’s resource commitment in this space is to prevent physical harm to young victims. In the United States (US), at least 12 child suicides were directly attributed to international sextortion in 2022 – this number is expected to grow (US national suicide rate within the young male target age group grew 8% nationally in 2022).

Prevention and Education Measures to Combat Child Sexual Exploitation

139. To combat child sexual exploitation the AFP and AFP-led ACCCE have a range of prevention and education measures that work towards ensuring all children are free from exploitation.

ThinkUKnow

140. The ThinkUKnow program has been delivered across Australia for more than 14 years, educating parents, carers and teachers about online child sexual exploitation and how to keep children and young people safe online.

141. The program is pro-technology and addresses topics including self-generated CAM, online grooming, sexual extortion and importantly encourages help seeking behaviour.

142. Since its inception, the scope of the program has expanded to include a suite of education materials including presentations, resources for parents, carers and teachers including toolkits, home learning activities, fact sheets and guides.

143. Through the ThinkUKnow program, the AFP holds the only capability in Australia that sees intelligence, examples from police investigations and victim reports of online child sexual exploitation developed into educational resources that are delivered to the Australian community.

144. The Online Child Safety Team works alongside operational teams including the ACCCEs Child Protection Triage Unit and Intelligence Fusion Cell and the AFP and state and territory police Joint Anti Child Exploitation Teams to develop this evidence-base and ensure that the program addresses online safety issues in a contemporary way.

145. In the 2022-2023 financial year, the AFP, state and territory police and industry volunteers delivered 257 presentations to an estimated 17,756 parents, carers, and teachers across Australia, including a mix of face-to-face and virtual sessions.

146. In the 2022-2023 financial year, the AFP and state and territory police also delivered 2,515 presentations to an estimated 209,544 students (Kindergarten/Prep – Grade 12) across Australia.

147. The AFP has seen an increase in demand for the ThinkUKnow program through delivery of presentations, and number of police members and industry volunteers being trained to deliver the presentation. The demand shows the need for education on online child sexual exploitation, and the important role the ThinkUKnow program plays in the community.

148. The program is a partnership with the AFP, Commonwealth Bank of Australia, Datacom and Microsoft Australia, and in collaboration with all state and territory police and Neighbourhood Watch Australasia.

149. The ThinkUKnow program highlights the importance of partnerships across law enforcement and industry, working together to help keep children safer online.

Operation Huntsman (financial sextortion) awareness and education initiatives

150. Operation Huntsman was created to combat the increasing threat of sexual extortion (also known as sextortion).

151. In response to this increasing threat and reports, the AFP (ACCCE and ThinkUKnow) commenced an awareness and education package that included:

- Media releases to increase awareness of financial sextortion and Operation Huntsman.
- ThinkUKnow ‘Online blackmail and sexual extortion response kit’ for young people aged 13–17 on how to recognise sexual extortion, manage online incidents, report and get help.

- Email safety message from the AFP and ACCCE to all Australian high schools in December 2022 advising of the global sextortion trend and providing them with a student poster, information for families, what they can do and where to get further information.
- Email advice to all Education Departments in Australia advising the AFP would be writing to all high schools with an urgent safety messaging about the global sextortion trend.
- Creation of a dedicated web page on the ACCCE website with information on sextortion, how to get help and report, and resources available for victims.
- Development of awareness posters for display in schools, police stations and financial institutions with a QR code to report to the ACCCE.
- Youth targeted advertising on social media platform Snapchat, including the creation of an animation on how to recognise sextortion and report to the ACCCE.
- Sextortion messaging kit for stakeholders, schools, parents and carers and organisations that work with young people.
- Ongoing social media accounts via AFP, ACCCE and ThinkUKnow targeting parents and carers.
- Engagement with mental health services and support services to discuss victim support, messaging and training.
- Engagement with education sector, including education departments, to deliver webinars for educators, parents and carers.

Child Protection Children's Book – Jack Changes the Game

152. The AFP recognises that prevention and engagement is important for all ages in order to fight the cyber-enabled crime of child sexual exploitation.

153. Jack Changes the Game is a book that helps children recognise the signs of online grooming and understand the importance of getting help, support and making a report to police.

154. This is a first-of-its-kind resource developed by law enforcement for teachers, parents and carers to read with 5 to 8-year-old children.

155. The book is based on a real report to the ACCCE and shows a common situation of a child being approached while playing a game online.

156. The resource was developed in collaboration with a reference group comprising some of Australia's leading experts in child protection, with funding provided by the Commissioner's Innovation Fund.

157. The book is supported by a ThinkUKnow learning package with lesson plans and home activities.

158. Printed copies of Jack Changes the Game were distributed to approximately 8,500 primary schools nationally in December 2022, and the eBook has been downloaded from the ThinkUKnow website more than 20,000 times since release (between October 2022 and 30 June 2023). Options are being explored for an online interactive eBook.

159. Jack Changes the Game was recently recognised by the Queensland Child Protection Week Awards 2023, winning the Education Initiative Award, acknowledging its outstanding contribution to child protection.

Look a Little Deeper

160. The AFP has observed that technology combined with the reopening of national and international borders post COVID lockdowns is increasing, enabling and amplifying human exploitation, including human trafficking and slavery. Cybercrime is intersecting with human trafficking to a greater extent as offenders increasingly use modern communication technologies to exploit their victims.

161. Technology and the internet – both cybercrime tools – have made it easier for offenders to locate, recruit, coerce and control their victims.

162. The AFP is aware of individuals using technology and deceptive methods to recruit and exploit persons from overseas. For example, the AFP has investigated reports of forced marriage where online chat technology was used to ‘groom’ victims into marrying persons in Australia, where victims may be promised a better life in Australia, but upon arrival to Australia, the victim may find themselves living in servitude like conditions.

163. Similarly, the AFP is aware of instances internationally where technology has been used to facilitate a practice called ‘live begging’, where the victim is coerced by a perpetrator into performing certain actions online, with a goal of eliciting payment from unsuspecting victims.

164. Offenders are also facilitating forced labour ‘call centres’, where multiple victims work under forced labour and slavery-type conditions. The victims are coerced into committing offences themselves by engaging in online or telephone scams against other victims for money which goes to the facilitator. This crime phenomenon has grown to such a large-scale and spread across numerous countries that the international policing agency INTERPOL has established ‘Operation Storm Makers’, a co-ordinated operation targeting migrant smuggling and human trafficking.

165. The AFP’s training and awareness program, entitled “Look-a-Little-Deeper” (LALD) is designed to raise awareness amongst state and territory police and other Commonwealth agencies on the different types of human trafficking offences and trends to help them recognise the subtle warning signs and indicators of human trafficking and slavery type offences in the community.

166. The LALD program was nationally launched to front line responder agencies in 2021 and is the first unified training and awareness-raising program to be delivered to all frontline agencies and jurisdictions. The program ensures enhanced capability of frontline officers and first responders, and a consistent approach nationally.

167. During 2022, in partnership with the United Nation (UN) Global Compact Network Australia, the AFP delivered a number of LALD sessions to their Modern Slavery Community of Practice. These sessions were aimed at assisting companies by raising awareness of human trafficking and slavery indicators, understanding the investigation process and assisting companies designing and developing their modern slavery response plans.

Challenges and Opportunities

168. As technologies continue to advance and create new capabilities, it brings forth new challenges for law enforcement to ensure we are aware of new methods and tools used by criminals to exploit victims.

169. Australia will almost certainly remain an attractive target for cybercriminals, due to extensive internet connectivity, increasing reliance on the internet and our relatively high per-capita wealth.

170. However, while technological advances bring new challenges, they also present new opportunities for law enforcement. In order to stay ahead of cyber criminals, it is imperative law enforcement are adequately skilled and resourced.

171. The AFP is focussed on meeting the threats and opportunities posed by technology. The challenge of countering new threats requires continual investment in technology by law enforcement, supported by training and robust governance to enable a technically literate and empowered workforce.

172. The AFP is continuing to enhance cybersecurity capabilities with a focus on leveraging technology. The focus is to enhance the AFP's ability to detect, analyse, coordinate and provide effective response to high-volume, high-impact cybercrime that pose a significant threat to Australians and the Australian economy.

173. While attracting and retaining experts with the necessary specialist skills continues to be a challenge for all Commonwealth government agencies, the AFP continues to develop innovative ways to attract people to the organisation, and is dedicated to ensuring continuous training, development and opportunities for upskilling.

174. Private sector engagement remains crucial to increase the visibility of threats and trends to inform prevention and mitigation efforts while whole-of-government cooperation will ensure that information and resources are leveraged to their greatest capacity.

Case Study – Operation BIRKS

Operation BIRKS is a joint AFP and Australian Securities and Investments Commissioner (ASIC) investigation into a series of actual and attempted compromises of the superannuation and share trade accounts of multiple Australian victims.

Operation Birks was undertaken:

- In consultation with the Australian Tax Office-led Serious Financial Crime Taskforce (SFCT), a joint-agency taskforce which brings together multiple Government agencies, both domestically and internationally to share information and identify criminals, using the knowledge, resources and experience of relevant law enforcement and regulatory agencies to address the most serious forms of financial crime.
- With strong support and assistance from the Australian superannuation and share fund industries.

The crime syndicate acted both within Australia and offshore using a combination of cyber-offending methods, including phishing emails and spoof websites, to gain unauthorised access to superannuation accounts and share portfolios belonging to Australians.

All victims had PII stolen which was then used in the creation of online fraudulent identities to facilitate the offending. Stolen money was laundered overseas, primarily to Hong Kong, with proceeds of these crimes then disbursed back to Australian criminal syndicate members via a range of mechanisms including cryptocurrency.

In September 2019 the primary Australian-based facilitator was arrested in Victoria and has since been sentenced to five years and six months' imprisonment with a non-parole period for her central role in a major international criminal syndicate, which stole millions of dollars from the superannuation and share trading accounts of innocent victims using fraud and identity theft.

The offender worked with others to create a cloned website that mimicked the legitimate website of a superannuation fund, using a domain name that was almost identical to the legitimate site. Online advertisements were used to promote the cloned website to bring it the top of the search engine. The intention was to harvest members' usernames and passwords when they visited the cloned website ('phishing'). The stolen member information was used to gain unauthorised access to member accounts.

The syndicate withdrew the superannuation savings of victims and deposited them in the fraudulent bank accounts. The stolen funds were laundered by sending them to an overseas contact, who used the funds to purchase untraceable assets such as jewellery and luxury brand items in Hong Kong. These were then sold and the money remitted to the offender in Australia through cryptocurrencies.

The amount stolen through the fraudulent scheme is estimated to be in excess of $3.3 million and attempts were made to steal an additional $7.5 million from the victims' super and share accounts. More than 5000 of stolen identification documents were used and 17 Australian of organisations were breached.

The group laundered an additional $2.5 million through the purchase, and on-selling, of luxury goods in Hong Kong.

Artificial Intelligence (AI) Challenges

175. Current trends such as Ransomware-as-a-Service (RaaS) and Malware-as-a-Service (MaaS) reflect a lowering of the barrier to entry for cybercriminals who may lack the resources or technical proficiencies to develop their own cybercriminal capabilities.

176. The frequency and severity of cybercrime incidents are expected to increase as a result, placing new demands on the AFP as a law enforcement agency.

177. Malicious Artificial Intelligence (AI), are generative AI models with monikers such as FraudGPT and *WormGPT*. They provide a suite of Cybercrime-as-a-Service (CaaS) tools such as crafting spear phishing emails (with perfect grammar and spelling) and vishing (voice phishing/Hi Mum, Hi Dad scams), Business Email Compromise attacks, generating malware, exploit scanning and target acquisition.

178. Evidence of malicious AIs emergence indicates activity on dark web forums and encrypted channels since July 2023.

179. The development of malicious AI models by threat actors is in its early stages, but are already proving effective and lower the entry threshold for burgeoning cybercriminals who may lack the technical proficiencies or resources to establish their own cybercriminal tradecraft.

180. Malicious AI demonstrates an evolution in the 'Cybercrime-as-a-Service' business model, leveraging open-source AI large-language models to reduce development time, provide bespoke tradecraft, and lowering the barrier to entry for cybercriminals.

181. Malicious AI uses also include generating increasingly realistic deepfakes, life-like CAM, and believable disinformation content.

182. AI is an emerging technology in child exploitation matters and as it improves, the material is becoming more life-like. This type of material is known as deepfakes, which involve manipulating images, audio and video using AI.

183. While the AFP cannot comment on specific cases involving AI generated child sexual abuse material, law enforcement in Australia and international jurisdictions are starting to see this type of material and are monitoring the quality and characteristics of AI-generated content that may be relevant to AFP operations.

Artificial Intelligence Opportunities

184. The AFP is exploring opportunities to use AI to assist with the investigative processes, advanced data analytics and improve early threat detection of cyber threats.

185. The AFP has made a public submission in response to the Department of Industry, Science and Resources public consultation on safe and responsible AI in Australia. The submission

reaffirmed our resolute commitment to addressing the threats and opportunities posed by AI, including how we will work towards ensuring responsible and ethical innovation in this space.

186. Our vision is to combine the strength of AI and human expertise, ensuring accountability, responsibility and transparency.

187. The AFP recognises AI is another tool, and it will not replace the requirement for a person to remain accountable for any decision that impacts on the rights of another person. Policing is deeply connected to society and must reflect the values, norms and expectations of the community it serves.

188. The agreement on the ANZPAA AI Principles by all Australia and New Zealand Police Commissioners is foundation to this and our immediate focus will be building guardrails and governance to operationalise these guided principles.

189. Investments in AI will propel our organisational capabilities, enabling us to address a changing threat environment harming Australians and Australia's way of life. Managed correctly, the AI will offer the AFP opportunities to:

- create operational efficiencies;
- improve situational awareness to inform better human decision making, and;
- minimise risks to public safety, AFP members and capabilities;
- AFP Usage of AI.

190. The AFP's current use of AI has generally been limited to facilitating the transformation of data from one format to another, to enhance analysis and processing needs.

191. AI tools such as Chat GPT present the AFP with an opportunity to simplify the task of identifying potential value from large lawfully collected datasets. By speeding up the discovery task, members can make decisions earlier and execute the necessary actions accordingly.

192. The AFP is working collaboratively with State and Territory Police, Commonwealth agencies, academia and industry, to lead a dialogue on the safe and responsible utilisation of AI within the domains of law enforcement.

193. The AFP will also leverage existing structures such as the ANZPAA, FELEG, Interpol and Europol to assess governance frameworks, address global AI complexities, and sector specific utilisation.

Anonymising Technologies

194. While the AFP supports privacy and information security, anonymising technologies are exploited by criminals to avoid detection and access by law enforcement.

195. In 2021-22, 94% of internet data lawfully intercepted by AFP was unintelligible due to the use of encryption.

196. The AFP is developing innovative ways to address this issue including by using new powers such as Computer Access Warrants introduced by the *Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018* (TOLA) and the 3 new warrants introduced by the SLAID Act.

Future Legislative Reform

197. As the Commonwealth's principal law enforcement agency, the AFP can provide valuable insights into current legislative frameworks for criminal offences and law enforcement powers. As the current cybercrime operating environment continues to evolve, so too must the powers and offences available to law enforcement.

198. Legislation to address cybercrime, particularly new or amended offences, must be technology-neutral and future proof. If too closely reflective of specific criminal methodologies or currently-available technology there is a risk that any reforms may be swiftly outdated, or rendered ineffective by the pace of technological change. The technology-neutral drafting of the current offences in Part 10.7 of the *Criminal Code* is therefore an advantage.

199. However, many of the cybercrime offences in the *Criminal Code* (particularly Part 10.7) have not been updated since their introduction in the early 2000s. As such, the AFP supports and is engaged in the review being undertaken by the Attorney-General's Department of the cybercrime offences in the *Criminal Code* to ensure modern challenges in the cybercrime environment are adequately captured.

200. Finally, reforms which better enable information sharing between Commonwealth, State and Territory partners, particularly where information has been gathered by the AFP pursuant to Commonwealth powers (such as Computer Access Warrants, surveillance devices or interception) would also be beneficial, noting the borderless nature of cybercrime.

Conclusion

201. The AFP is committed to protecting lives, protecting livelihoods and protecting Commonwealth interests.

202. Cybercrime remains a complex and fast-paced crime and the AFP is committed to responding to the rising challenge.

203. In responding to the increased complexities of this multifaceted issue, we acknowledge that we cannot do it alone and look forward to our continued cooperation and collaboration with Commonwealth and state and territory agencies, industry and NGOs.

Attachment A- AFP Engagement in Cybercrime Related Forums

Forum	Purpose
Australian New Zealand Policing Advisory Agency (ANZPAA) Board	ANZPAA Board comprises Commissioners of the policing agencies of each Australian jurisdiction and New Zealand.
Australian Transnational Serious Organised Crime Committee (ATSOCC)	A national forum attended by Deputy Commissioner representatives of policing agencies from each Australian jurisdiction and New Zealand, and deputy agency head level representatives from Justice or Attorneys-General agency, New Zealand Ministry of Justice, ACIC, AUSTRAC, the Office of National Intelligence and the Department of Home Affairs and Australian Border Force. Established to drive implement and monitor the National Strategy to Fight Transnational, Serious and Organised Crime, the mission of ATSOCC is to build on understandings of current and emerging transnational, serious and organised crime (TSOC) threats and enablers and provide strategic and policy advice to ministers on national priorities to combat TSOC, including addressing cybercrime.
Serious Organised Crime Coordination Committee (SOCCC)	The SOCCC is a national committee that prioritises, endorses and coordinates operational strategies to address serious and organised crime investigations. Membership is at Assistant Commissioner (Crime) level, and includes representatives from all Australian police jurisdictions, New Zealand Police, ACIC, AUSTRAC, Australian Taxation Office and Department of Home Affairs. Cybercrime working group, Op Helios, reports to the SOCCC.
Op Helios	A working group comprising cybercrime representatives from each Australian jurisdiction and New Zealand Police, Attorney-General's Department, Australian Signals Directorate, and the Australian Criminal Intelligence Commission. The purpose of the working group is to prioritise and coordinate operational capability and strategies to combat cybercrime, including multi-jurisdictional investigations, de-conflicting operations, and disrupting cybercriminals.
Strategic Cybercrime Operations – Joint Management Group (SCO-JMG)	Comprising Assistant Commissioner-level chaired forum including representatives from AFP, ASD and ACIC. SCO-JMG is responsible for ensuring strategic direction to the Operations Coordination Group (OCG) and will consider

	strategic cybercrime operational priorities to provide guidance, priority setting and direction to the OCG.
Strategic Cybercrime Operations – Operations Coordination Group (SCO-OCG)	Established to plan, coordinate and oversee operations against cybercriminal syndicates, and their enabling entities, as endorsed by the Strategic Cybercrime Operations Joint Management Group (SCO-JMG).
Joint Policing Cybercrime Coordination Centre Board of Management (JPC3 BoM)	The JPC3 BoM includes contributing agencies to the JPC3 and provides oversight on JPC3 success and progress.
Joint Policing Cybercrime Coordination Centre Steering Committee (JPC3 SC)	The JPC3 SC provide strategic guidance, operational advice between partners and ensuring the prioritisation of resources to achieve the objectives of the JPC3.
Five Eyes Law Enforcement Group Cybercrime Community of Practice (FELEG CCoP)	The FELEG CCoP is an international working group whose activities include assessment of the cybercrime ecosystem, and alignments between law enforcement and other partners in counter cybercrime efforts.
International Cyber Crime Operations Group (ICCOG)	The ICCOG provides coordinated strategic level law enforcement response to priority cybercrime threats across member nations. The National Cyber Crime Unit (UK) currently chairs this forum.
Joint Cybercrime Action Taskforce (J-CAT)	The J-CAT aims to steer the cybercrime taskforce, set strategic direction, validate working procedures and make decisions to address strategic matters. The forum was established and is chaired by the European Cybercrime Centre (EC3).