10 January 2024

AFP Submission to the Commonwealth Government COVID-19 Response Inquiry

Independent inquiry into Australia's response to the COVID-19 pandemic.

AFP

afp.gov.au

Table of Contents

Introduction 2
AFP role and operational response 2
AFP organisational response 5
Collaboration and partnerships 6
Intelligence and crime trends 9
Challenges 13
Conclusion 14

Report details

Date produced	5 December 2023

Introduction

The Australian Federal Police (AFP) welcomes the opportunity to make a submission to the *Independent inquiry into Australia's response to the COVID-19 pandemic.*

The AFP is the Commonwealth's national law enforcement and policing agency and remains committed to our vision of policing for a safer Australia. The AFP's remit is broad focusing on national security, enforcement of Commonwealth criminal law, specialist protectives services, international police cooperation and assistance, and community policing in the Australian Capital Territory (ACT) and Australia's external territories.

The AFP continues to focus its activities on protecting lives, livelihoods and Australia's way of life and maximising our impact on the criminal environment. Despite international and domestic border closures, lockdowns and illness, the AFP successfully responded to a number of new crime threats and policing challenges.

AFP role and operational response

The COVID-19 pandemic altered demands on police nationally, with changes to the criminal landscape providing new opportunities for criminals to exploit Australians and Australian interests. Nationally, Australian policing agencies adapted swiftly to the changing criminal landscape and operating environment to prevent, disrupt, investigate, and resolve crime while protecting their own personnel and the Australian community.

COVID-19 changed the operational tempo for the AFP as we saw an increase in victim based crimes across the country including online child sexual abuse and the targeting of young people online. During the pandemic the AFP prioritised activities to protect the community in Counter-Terrorism, Aviation, Protection Operations and ACT Community Policing.

Additionally, the threat landscape evolved in response to enforcement of mandated COVID-19 restrictions, resulting in an increase in issue-motivated activity from individuals espousing anti-authoritarian rhetoric. This included anti-Government and anti-police sentiment and protests by individuals and groups not previously known to law enforcement, posing additional challenges for police.

Operation BURDEI

On 2 February 2020, the Australian Government implemented additional border measures to manage the entry to Australia of people who had departed or transitioned through mainland China. In response, the AFP established Operation BURDEI to assist the Australian Border Force (ABF) with the repatriation of Australians returning from China and Japan.

The AFP deployed 52 officers to Christmas Island, Learmonth and Darwin to assist the repatriation operation including the successful transfer of passengers via charter flight from Wuhan, China to Christmas Island for quarantine purposes. Operation BURDEI was deactivated on 5 March 2020.

Operation PROTECT

On 5 March 2020, the AFP established Operation PROTECT, the AFP's emergency response to the COVID-19 pandemic. This involved a 24/7 AFP Incident Coordination Centre (ICC) to coordinate the AFP's efforts and contributions to the Whole-of-Government response to COVID-19.
Operation PROTECT consisted of three key pillars of focus: protecting our people, safeguarding Australia's national interests, and assisting with public safety.

Joint Intelligence Group

On 19 March 2020, the AFP established the Joint Intelligence Group (JIG) as the central point of intelligence in support of Operation PROTECT. The role of the JIG was to determine potential risks to Australia from all crime types, including economic and financial crime; transnational, serious and organised crime; cybercrime; espionage and foreign interference; human trafficking and child exploitation; and terrorism. The JIG coordinated efforts across Australian law enforcement, intelligence agencies and international partners, to provide timely and informative advice to assist decision-making.

The JIG disseminated a number of operational and strategic intelligence products. These products were informed through daily intelligence and reports received by state and territory policing, the Department of Home Affairs, Australian Border Force (ABF), Australian Criminal Intelligence Commission (ACIC), Australian Transaction Reports and Analysis Centre (AUSTRAC) and New Zealand Police. COVID-19 operational and strategic intelligence products were then disseminated broadly with JIG members to ensure situational awareness and to inform decision making.

As the COVID-19 pandemic and community response evolved so did the law enforcement focus. The JIG continued to operate with partner agencies to collect and share intelligence in relation to COVID-19 vaccine related criminal activity, and fraudulent/counterfeit COVID-19 polymerase chain reaction (PCR) test results and vaccination certificates. The AFP was also a member agency of Operation HANGFIRE BRAVO, an ABF operation focused on detecting unapproved, substandard, counterfeit or contaminated critical consumables and counterfeit medical equipment associated with COVID-19. The intelligence support to the importation (and related issues) of the COVID-19 vaccines was provided by the JIG and Joint Analyst Group (JAG), of which the AFP was a participating agency.

COVID-19 Counter Fraud Taskforce – COVID payments fraud

The COVID-19 Counter Fraud Taskforce was established on 27 March 2020 by the AFP and the Attorney-General's Department (AGD) to support Commonwealth efforts to mitigate serious and complex fraud targeting Australian Government COVID-19 economic stimulus measures. The Counter Fraud Taskforce developed a coordinated action plan with 19 key activities across four objectives:

- support policy, program and system design to counter fraud activity;
- identify fraud risks and controls;
- develop information sharing and intelligence arrangements across government to maximise the ability for agencies to prevent, detect and disrupt fraud; and
- Promote deterrence through strategic messaging about the government's preparedness to prevent, detect and respond to fraud.

To enhance the integrity of processes, the COVID-19 Counter Fraud Taskforce provided guidance on mechanisms such as fraud clauses in legislation and minimum standards for data collection to enable post-payment compliance activity and recovery. As part of the COVID-19 Counter Fraud Taskforce, the AFP produced 14 *Fraud in Focus* intelligence papers and established the Operational Intelligence Group bringing together ten Commonwealth agencies to share intelligence on fraud and develop fraud detection strategies. The Taskforce ceased on 30 June 2020.

Taskforce QUADRANT

On 28 March 2020, the AFP established Taskforce QUADRANT in partnership with ABF, ACIC and AUSTRAC. Taskforce QUADRANT focused on suspected breaches of the Health Minister's determination under the *Biosecurity Act 2015* and the amended *Customs (Prohibited Exports) Regulations 1958* relating to the improper export and/or profiteering from price gouging on essential goods. Taskforce QUADRANT engaged in overt deterrence and compliance activities across Australia, including educating businesses and entities about their requirements in dealing with essential goods under this Determination.

Taskforce IRIS and Taskforce LOTUS

On 27 April 2020, the AFP established an Anti-Fraud Investigations Taskforce to target persons and organised crime entities who planned to defraud the Governments COVID-19 stimulus measures. Taskforce IRIS worked closely with partner agencies, including Australian Tax Office (ATO), Services Australia, Australian Securities Investments Commission (ASIC), Australian Consumer and Consumer Commission (ACCC), Australian Prudential Regulation Authority (APRA), AUSTRAC and ACIC. Taskforce IRIS resulted in 17 persons charged, with a combined total of 141 offences. On 1 December 2020, Taskforce IRIS ceased as a separate Taskforce and was rolled into AFP business as usual. Taskforce LOTUS

On 8 February 2021, the AFP established Taskforce LOTUS as a targeted, scalable response to potential criminal threats to the COVID-19 vaccine rollout, including emerging frauds and scams related to COVID-19 vaccination status and records. The AFP assisted Commonwealth, state and territory partners to investigate multi-faceted COVID-19 crimes. For example; diverted, fake or counterfeit vaccines; unregistered imports of Rapid Antigen Tests (RATs); sale of positive RATs to support claims for COVID-19 payments; fraud against Commonwealth procurements and grants; fraudulent vaccination certificates; and the manipulation of the Australian Immunisation Register to falsely record individuals as having received the vaccination.

On 8 January 2022, the Health Minister issued a new Determination under the *Biosecurity Act 2015* in response to allegations of price gouging of RATs. The ACCC was responsible for receiving allegations of inappropriate and unconscionable consumer activities, which included price gouging, importing and the sale of unregistered RATs, package splitting, no instructions, cash sales and no or incorrect receipts related to rapid antigen tests, with allegations of price gouging referred to the AFP where appropriate.

Reports received by the AFP from members of the public that related to potential breaches of Australian Consumer Law were referred to the ACCC and potential breaches of the *Therapeutic Goods Act 1989* referred to the Therapeutic Goods Administration for their consideration.

AFP organisational response

The AFP has an obligation to ensure a safe workplace for all AFP Appointees. Due to the AFP's public safety role, it is also imperative to maintain a workforce capable of delivering its functions and statutory duties. The AFP's role in interacting with the public created an additional level of complexity in protecting the health and safety of its workforce. The AFP takes risk to its members and to vulnerable communities seriously. To mitigate the risks, the AFP implemented social distancing and other precautionary measures in the workplace, consistent with advice from health authorities.

On 4 March 2020, the AFP established a dedicated 24/7 hotline, staffed by in-house clinicians, to provide COVID-19 related advice to AFP Appointees and their families. AFP clinical staff undertook in-house contact tracing to determine and minimise the spread of COVID-19 within the workforce, which resulted in low case numbers within the AFP and ensured continuity of operations.

Mandatory vaccinations

On 29 October 2021, the AFP issued the *Commissioner's Order on COVID-19 Vaccination* (CO10) and the *AFP National Guideline on Mandatory COVID-19 Vaccination* which required all AFP employees to be fully vaccinated against COVID-19, unless exempt. The decision to introduce CO10 was carefully considered and informed by operational risk. The AFP consulted with the workforce on the decision to issue CO10, including through the AFP Health and Safety Committee. AFP also considered advice from Australia's Chief Health Officer and the Department of Health when making the decision.

Mandating vaccination was considered necessary to protect our people and provide a safe working environment as well as to protect the community we serve. In late 2022, following an updated COVID-19 risk assessment, the AFP considered the requirements within CO10 and whether it continued to meet the needs of the AFP and be commensurate to the operating environment. Following the 2022 updated risk assessment, the AFP decided that two primary COVID-19 vaccinations will continue to be a requirement, while booster doses are strongly encouraged (in line with Government recommendations). The 2022 update to requirements recognises the prevailing community expectations of the AFP to protect its workforce and the community against COVID-19. In reaching this decision, the AFP consulted with expert practitioners, health and safety representatives, employee representatives and the workforce more broadly.

Personal protective equipment

All frontline, airport and internationally-based AFP Appointees were provided with significant amounts of personal protective equipment (PPE) by early February 2020. The AFP planned and managed a consistent supply chain for the purchase, storage and provisioning of PPE.

Rapid antigen testing

The AFP provided point-of-care RATs at all AFP workplaces. The RATs were distributed across workplaces in Canberra (including ACT Policing), and in workplaces across the states and territories. The AFP invoked a model of workplace testing, including a hybrid of self-detection and approved person-led testing. The adoption of RATs increased operational efficiency through easier access to testing, particularly by those frontline and other members requiring frequent testing.

Working from home and flexible work arrangements

The AFP implemented a COVID-19 Workforce Reintegration Plan to manage the transition of staff back into the workplace as local conditions changed as a result of COVID-19. The plan covered working from home, social distancing, travel, meetings and personal protection arrangements. The AFP continues to recognise the importance of flexible work in attracting and maintaining a diverse and engaged workforce and is committed to creating a workplace where employees are supported in managing their work and personal commitments.

Supporting AFP members at International Posts

AFP members remained posted internationally and continued their valuable work with partners. The AFP developed and applied a risk matrix considering the welfare of our officers, offshore health protocols and infrastructure and our ongoing commitment to our international partners. The risk in each of our international locations was assessed and updated regularly. AFP also engaged weekly with all international posted officers and continued to action intelligence, operational and best practice requests and advisories to/from foreign partners including INTERPOL and Europol. Throughout the COVID-19 pandemic, foreign law enforcement agencies primarily focused on domestic challenges which included support to the health crisis within their jurisdiction. Although this resulted in existing priorities being re-focussed and engagement limited or narrowed, the AFP adopted a risk-based approach to maintaining our members in place offshore to continue supporting our foreign law enforcement counterparts. The AFP considered its engagement internationally to be critical to achieving outcomes for the Australian Government.

Collaboration and partnerships

Throughout the COVID-19 pandemic, Australian law enforcement agencies worked closely to identify domestic and national vulnerabilities, and closely monitored and managed changes in their operating environment, in particular criminal behaviour. Close national cooperation is a strength of the Australian policing landscape. These relationships facilitated the effective national policing response in support of the broader efforts by governments nationally which kept Australians safe and minimised the spread of COVID-19.

During the outbreak of COVID-19, Commonwealth, State and Territory, and New Zealand Police Commissioners met regularly – weekly during the peak of the initial outbreak - to align efforts, share experiences and best practice, to ensure mechanisms were in place to protect staff and preserve operational capability and capacity. The Deputy Commissioners Operational Management Meeting network was used to collaborate and coordinate operational responses to national issues, ensuring timely and appropriate responses to emerging issues, forecasting and planning.

The National Coordination Mechanism (NCM), led by the Department of Home Affairs, was activated on 5 March 2020 to coordinate and facilitate Commonwealth, state and territory COVID-19 planning and preparedness in non-health sectors. The NCM was rapidly stood up and effectively addressed the gap in existing crisis management arrangements.

The AFP cooperated closely with a range of agencies to administer the stringent border controls implemented nationally and internationally during the pandemic, particularly at airports. Substantial collaboration between the AFP and state/territory police, health departments, ABF,

Australian Defence Force (ADF) and airport operators took place, to ensure the integrity of quarantine arrangements, particularly as they applied to international repatriation flights.

The COVID-19 pandemic also highlighted the strength of AFP's partnerships with industry and non-government organisations, particularly in spheres of child exploitation and online safety.

Assistance to Northern Territory Police Force

On 23 March 2020, the Northern Territory Police Force (NT Police Force) advised the AFP of plans to implement border control measures across Northern Territory borders on 24 March 2020 and requested AFP assistance. From March 2020 to January 2021, the AFP deployed a total of 196 Police and Protective Service Officers to the Northern Territory to work alongside the NT Police Force. AFP officers supported NT Police Force to prevent the spread of COVID-19 into remote Aboriginal communities in the Northern Territory classed as 'specified areas' under the *Biosecurity Act 2015* (Cth), by controlling access into those specified areas. AFP members were deployed to 14 locations throughout the Northern Territory to implement biosecurity and border control checkpoints. AFP members were also deployed to support the NT Police Force at the Howard Springs International Quarantine facility under Operation Protect-Assist.

ACT Policing and external territories

During the pandemic, ACT Policing was responsible for providing quality and effective community policing services in partnership with the community and ACT Government. ACT Policing commenced their response to the COVID-19 pandemic when the declaration of the public health emergency and health directions were issued. ACT Policing established a dedicated COVID-19 Taskforce in July 2020 to ensure a centralised, coordinated response to business continuity, safeguarding community health outcomes and enforcement action.

ACT Policing's resources were bolstered in response to the 12 August 2021 lockdown. At its peak, approximately 110 members were attached to the COVID-19 Taskforce. This included compliance teams, administrative support, embedded officers liaising with partner government agencies, and a command structure. Sworn members were largely redeployed from areas such Community Engagement Team, Education and Diversion Team, Proactive Intervention and Diversion Team, Territory Targeting Team, Criminal Investigations and General Duties.

The focus of ACT Policing's response to COVID-19 required the effective redirection of AFP Members, however, priority investigations continued. The command structure also expanded with the introduction of a dedicated COVID-19 Commander to oversee ACT Policing's response to the threat of the pandemic. Resources attached to the COVID-19 Taskforce fluctuated throughout the pandemic depending on the threat that was posed to the community. All operational members attached to the COVID Taskforce were released by March 2022, with compliance activities forming part of business as usual for all ACT Policing members.

Each and every day, ACT Policing prioritises calls for help to ensure police support is directed to incidents that required immediate attention and the highest threats to public safety. The approach during the COVID-19 pandemic was no different. Police also made an effort to operate safely– for example, when ordinarily patrols may have attended a person's residence to follow up on a non-urgent matter, a phone call was made instead so the engagement could continue in a safe way.

As a result of the closure and restrictions of restaurants, night clubs, schools and public gatherings, the requirement for ACT Policing to undertake certain targeting, education and engagement with respect to these locations usually performed by the Territory Targeting Team,

Community Engagement Team, and Education and Diversion Team was reduced. This provided an opportunity for ACT Policing to redirect these members to the COVID-19 Taskforce.

Canberra Convoy Protests ACT

On 31 January 2022, AFP established Operation HAWKER to monitor, respond, ensure safety and move on trespassers on National Capital Authority land as part of a wave of protest activity requiring a large-scale police response. During the height of the protests in early 2022, ACT Policing was supported by the AFP resources from across the country. This was aimed to ensure an adequate police presence to respond to protest activity and to maintain community confidence.

Issue Motivated Groups arrived in Canberra spurred on by protests occurring internationally. These protest groups were largely motivated by a range of COVID-19 related issues including anti-vaccination mandates and COVID-19 restrictions. On 12 February 2022, there was a significant escalation in protest activity, with an estimated 10,000 protesters in attendance. As at 15 December 2023xxx, there had been 82 arrests made in relation to unlawful activity under Operation HAWKER.

External Territories

During the COVID-19 pandemic, AFP officers in the External Territories (Jervis Bay, Norfolk Island, Christmas Island and Cocos (Keeling) Islands) were integral to responding to and enforcing the Commonwealth, NSW and WA governments' requirements to prevent COVID-19 in these External Territories. The COVID-19 response in the External Territories was of particular importance due to difficulties with accessing medical assistance. Throughout the COVID-19 pandemic, AFP officers checked on members of the community who were in isolation to ensure they had enough food, water, medical supplies and entertainment to support their mental and physical health. These actions demonstrate the varied duties that ACT Policing and AFP officers undertook, responded and enforced requirements relating to COVID-19, which were in addition to their usual community policing roles. At all times, ACT Policing's focus was maintaining an Engage, Educate, Enforce approach, in line with ACT Government COVID-19 response.

Closing Police Stations

Police stations were open for urgent and time critical police matters. This included emergency support, violence occurring at the time, and importantly for people to report for bail. On 12 August 2021, a decision was made to shut the front offices of all police stations to mitigate risk to ACT Policing members and to align with the closure of other ACT Government shopfronts. Front offices were re-opened on 17 September 2021 after a risk assessment and mitigation plan was approved.

International assistance

The AFP's international presence continued during the height of the pandemic. The AFP had members deployed in 33 countries prior to COVID-19, and were able to maintain a comprehensive footprint in-country or in some instances remotely during the pandemic. The AFP contributed to whole of Australian Government contingency planning and was prepared to assist with the deployment of additional resources.

Intelligence and crime trends

COVID-19 was a dominant factor influencing the global crime environment between 2020 and 2022. Criminal entities and serious and organised crime groups demonstrated their ability to adapt their methodologies during the pandemic, to ensure their continuity, capability and relevance. Due to the diverse impact of COVID-19 within the community there were various crime trends that were observed during the different stages of the pandemic, including the post-COVID-19 landscape. As the impact of COVID-19 evolved, criminals (both opportunistic and organised crime entities and groups) adapted to the environment (restrictions and lockdowns) to enable their enterprises to be maintained.

During the COVID-19 pandemic, the AFP identified an increase in criminal activity on the dark web, cybercrime scams, misinformation and foreign interference, extreme right wing, human trafficking and modern slavery. Transnational and serious organised crime (TSOC) impacting Australia continued throughout the pandemic. TSOC groups are resilient and altered their business model throughout the pandemic, including by locally recruiting and increasing use of closed social media communication, to further their illicit drug and money laundering activities. The impact of TSOC within the Australian context did not diminish despite COVID-19 related domestic and global restrictions. Organised crime groups (OCGs) demonstrated their resilience and agility to remain active as they continued to influence the transnational movement of illicit drugs and other commodities into Australia. OCGs developed alternate methods and supply chains to facilitate their activities both domestically and internationally.

Disruptions to global supply chains required organised crime groups to pivot quickly to new methodologies. Drug importation via the aviation stream was severely impacted, while the cargo streams faced significant time delays and greater associated costs. Post COVID, criminal groups went back to what worked well pre-COVID, while maintaining productive innovations. The pandemic and associated lockdown measures almost certainly contributed to substantial shifts in the Australian drug markets. Drug consumption, as measured by the ACIC Wastewater drug monitoring program, decreased significantly in 2020-2021 across Australia's four major illicit drug markets – methamphetamine, cocaine, MDMA and heroin. Consumption of MDMA and cocaine, typically associated with social drug use, reduced the most due to the lack of events and socialisation occurring during the COVID-19 pandemic. The wholesale cost of illicit drugs reached record highs during the pandemic, fuelled by supply chain disruptions and difficulties importing into Australia. Money laundering organisations in Australia demonstrated resilience during restrictions to continue operating on behalf of organised crime groups.

International counterparts reported that vaccine wastage from supply chain disruptions would present an attractive opportunity to actors seeking to obtain vials, labels and packaging to sell, repurpose or create counterfeit goods. Vaccine-related criminal activity included:

- phishing scams targeting personal information,
- advertisements for illegitimate COVID-19 treatments and health products,
- scammers impersonating vaccine brokers,
- online sale of fraudulent COVID-19 test results certificates and vaccination certificates,
- sale of used vaccine vials, and
- sale and distribution of counterfeit COVID-19 vaccines.

Online child exploitation

Online child sexual abuse is becoming more prevalent, commodified, organised and extreme. The COVID-19 pandemic increased the opportunity for online child exploitation and abuse, with increased online activity on the dark web identified by the AFP-led Australian Centre to Counter Child Exploitation (ACCCE), consistent with trends observed by law enforcement partners. It is highly likely that travel restrictions during this period increased the demand for live online child sexual abuse. This level of demand has not subsided post-COVID-19.

The ACCCE brings together law enforcement, the public and private sectors and civil society to drive a national response to deter, disrupt and prevent child exploitation, with a specific focus on countering online child sexual exploitation. The operational tempo remained high throughout the COVID-19 pandemic. Throughout AFP and ACCCE observed the emergence of discussions on child exploitation sites, providing advice on how to establish relationships with children in the COVID-19 environment as a direct result of stay at home measures.

Monitoring and evaluation by the AFP and law enforcement partners identified a significant increase in child abuse material being downloaded as COVID-19 restrictions were implemented globally. The COVID-19 pandemic did not slow investigators, who continued to operate on the dark and clear net to keep children safe online. The AFP bolstered resources within the ACCCE Child Protection Triage Unit to address the increase in referrals received, which amounted to over 22,600 referrals in the 2020-21 financial year.

In response to the increased risk to children online during the COVID-19 pandemic, the ACCCE partnered with the AFP ThinkUKnow education program to develop a comprehensive community engagement strategy to educate parents, carers and influencers of children. With the suspension of face-to-face ThinkUKnow presentations, the AFP was flexible and innovative in addressing the challenges of children spending an increased time online. Initiatives included online sessions and resources, such as home learning activities and teacher toolkits, tailored to meet the requirements of the COVID-19 environment and support parent, carers and teachers through this time.

Operation ARKSTONE

Operation Arkstone commenced in early 2020, following receipt of a report by the ACCCE from the United States' National Centre for Missing and Exploited Children about an online user allegedly uploading child abuse material. Operation Arkstone investigators identified links through the online forums to alleged child sex offenders residing in Germany, France, Sweden, Ireland, Netherlands, Spain, Philippines, Denmark, Russia, Poland, United Kingdom, United States, Canada and New Zealand. 154 international referrals have been made as a result of this investigation. The cross agency collaboration with United States Department of Homeland Security Investigations (HSI) throughout Operation Arkstone resulted in the arrest of three men in the United States for multiple child abuse offences.

The AFP, its state and territory police counterparts and HSI worked tirelessly after each arrest to piece together information that identified more victims and the people allegedly abusing and exploiting them. This has been a multi-agency effort from our international and domestic policing agencies to disrupt domestic online network of alleged child sex offenders, who are accused of abusing and exploiting Australian children and recording the horrific crimes. The operational success of Operation Arkstone demonstrates that the AFP continued to deliver maximum impact to the criminal environment throughout the COVID-19 pandemic, to ensure the safety of the Australian community.

Cybercrime

Cybercrime causes severe harm to the Australian community. The AFP recognise that Australia is facing increasing, persistent and pervasive cybercrime threats targeting critical infrastructure, governments, industry and the wider community. 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.

An increase in cybercrime throughout the COVID-19 pandemic was attributable to an increase in online activity due to social distancing or as a result of increased public awareness from social media messaging of how to report scams and fraud activity. Cybercriminals evolved their narrative to exploit people's anxiety and desire for COVID-19 related information during the pandemic.

Operation LASION

The incidence of Australians falling victim to scams increased during the COVID-19 pandemic. One of the most notable scam types is phishing. Phishing is the practice of scammers sending out emails and SMS messages impersonating reputable businesses (such as banks or phone providers) to convince victims to release personal information such as passwords and credit card numbers.

In September 2021, an investigation began when AFP Cybercrime Operations investigators received information about suspicious website registrations suspected of being used to phish the customers of Australian telecommunications providers and financial institutions. The offender orchestrated multiple SMS phishing campaigns through which SMS messages were sent to hundreds of thousands of Australians. The SMS messages spoofed the domain names of legitimate institutions, aiming to siphon customers' personal credentials including usernames and passwords. Through this method, the offender obtained victims' personal information, which was used to access existing telephone and bank accounts and create new accounts without their knowledge.

Responding to the threat, investigators used intelligence and technological capabilities to identify and uncover online databases containing the details of over 20,000 Australian victims who had been subjected to the phishing scams. The uncovered databases contained information on victims' bank accounts, login credentials, shareholdings and home loans. With the information acquired from these credentials, the offender would have been able to undertake a range of fraud and identity theft related schemes. During the investigation it was discovered that the offender had allegedly managed to siphon more than $100,000 from the victims and steal the identity of over 5,000 people. The offender and an accomplice were arrested by AFP Cybercrime Operations investigators in November 2021.

Counter terrorism

Terrorism continues to pose an enduring, complex and diverse threat to the Australian community. The operational tempo remained high during the COVID-19 pandemic, with extremists taking advantage of the resulting isolation to target individuals, specifically young people, online.

The online environment has allowed violent extremists to magnify their impact, particularly during COVID-19, through the sharing of extremist propaganda and material from anywhere in the world. This was the case with both religiously motivated and ideologically motivated violent extremism.

The emerging threat required the AFP to pivot our engagement and collaboration to non-traditional stakeholders including increased engagement with education and health departments at all levels of government. The AFP continues to expand its investigative focus in this domain working collaboratively across international and domestic partners to assist in various prevention efforts, mechanisms and diversion processes when engaging youth.

There is an identified increase in the presence of Australian youth deemed at-risk of radicalisation. Some commonalities that have been identified between these investigations include diagnosis of a neuro-diverse or mental health condition, being raised in a disruptive, unstable or harmful environment, and experiencing social problems throughout their school life.

The process of youth radicalisation differs from adults. This is due to the unique risk factors and vulnerabilities associated with childhood and adolescence. Research indicates that Australian youth radicalised to violent extremism are influenced by several factors, which include social dislocation, peer influence, active engagement with extremism online, and triggering events.

Significantly increased time spent online due to the COVID-19 pandemic restrictions created an environment in which radical ideologies could become more 'normalised'. This has been particularly evident in young people who tend to present as mixed/unclear ideologies from engaging with a variety of extreme views/material online.

Individuals involved in ideologically motivated violence extremism are geographically dispersed, although there has been an increasing trend in rural communities, and use online platforms and material for their broad reach.

The AFP identified an increase in ideologically motivated groups sharing COVID-19 rhetoric online to reinforce their messaging. The AFP, in collaboration with state and territory partners, continues to monitor the national threat environment to identify behaviour that is in breach of Commonwealth laws

Espionage and Foreign Interference

Espionage and Foreign Interference (EFI) represents a serious threat to Australia's people, sovereignty, security, and the integrity of our national institutions. EFI and related offences are highly complex and sensitive, and require a specialised and coordinated response. The AFP is a member of the Counter Foreign Interference Taskforce (CFITF), jointly led by ASIO, which brings together the expertise, capabilities and powers of Commonwealth partner agencies to boost our ability to discover, mitigate, investigate and prosecute the threat posed by EFI activity in Australia.

The CFITF observed a change in methodology employed by state actors following the introduction of the EFI legislation in 2018 which was exacerbated by the COVID-19 pandemic. State actors sought to identify and employ proxies in Australia to undertake EFI activities on their behalf. State actors also increased their online activities, including through disinformation campaigns, for example, to spread alternative views or discredit an Australian Government position, as well as targeting of Australian's in a bid to recruit them in order to access sensitive or privileged information. The AFP worked proactively as part of the CFITF to identify and disrupt instances of EFI activity in Australia.

The AFP also worked throughout the pandemic in close collaboration with whole-of-government agencies as part of the then newly established 'All Source Fusion Cell', led by the Department of Home Affairs, to identify and assess all forms of malign information manipulation (misinformation, disinformation, and scams, including phishing, ransomware/malware) relating to COVID-19.

Fraud

The AFP plays a key role in whole of government efforts to detect, disrupt and respond to serious and complex fraud. As detailed under *2. AFP role and operational response*, the AFP worked proactively to mitigate risks and respond to attempts to target and exploit the Government's COVID-19 stimulus measures through various taskforces and operations. Criminal activity and exploitation in relation to fraud targeting the Commonwealth stimulus packages and benefits during this period required a joint law enforcement and Commonwealth agency response. The type of offending and methodologies used in relation to these fraudulent activities generally involved adapted capabilities, exploited by organised crimes groups and opportunistic entities.

The Australian Government implemented a range of economic stimulus measures to support the Australian economy and workforce during COVID-19. Due to the imperative for payments to reach recipients in a timely manner, fraud controls were adjusted, increasing the likelihood of fraudulent claims and payments. AFP Operation Ashiba focussed on identifying operational intelligence gaps, and disruption opportunities through engagement with Commonwealth departments and agencies delivering COVID-19 economic stimulus measures. The significant disbursement of government funds prompted a range of fraudulent behaviour, including by serious and organised crime groups and opportunistic fraud entities. Although some offending increased, the types of offending, and the methodologies offenders utilised, were not new, these included:

- phishing scams, and other scams targeting personally identifiable information (PII);
- targeting of the Early Access to Superannuation (EAS) scheme – including unauthorised use of the myGov system.
- increase in scams relating to the rapid procurement of PPE to comply with demand;
- Fraud relating to childcare providers, especially after the cessation of JobKeeper payment for child care providers.

Challenges

The burden of the extra workload over the COVID-19 period was felt by the AFP, in particular the frontline officers, who were required to enforce mandated COVID-19 restrictions. On an individual level, policing during the pandemic increased the risk of members contracting the COVID-19 virus through interactions with the public, as well as spreading the virus to family and friends.

The increased time spent at home and online by the community impacted on the crime environment. During the pandemic there was an increase in joint agency disruptions, where police action disrupted young people early in their path to radicalisation, resulting in some having ceased online narratives, while others have broken away from negative influences or participated in re-education programs. Even after COVID-19, violent extremists continue to use the internet and other technology—including readily available encrypted messaging applications and online message boards—to facilitate their activities. The anonymous and secure nature of these platforms pose challenges to intelligence and law enforcement agencies that are trying to stop terrorist attacks.

During the COVID-19 pandemic, the AFP witnessed an increase in protest activity occurring. The AFP observed an increase in nationalist, racially motivated and religiously motivated violent extremists and sentiments including persons and groups exploiting public fear to further their own agenda. This included spreading disinformation, conspiracy theories, and in some cases motivation to incite violence. This presented challenges for law enforcement who were

simultaneously enforcing increased measures imposed by Government, while also policing an unprecedented changing criminal environment.

Conclusion

The AFP will continue to remain adaptive and flexible during times of crisis. This will ensure that operational targeting and disruption of crime will always continue, even during times of uncertainty and a changing threat and operating environment.