6 November 2025

AFP Submission to the Parliamentary Joint Committee on Law Enforcement

Inquiry into Combatting Crime as a Service.

AFP

afp.gov.au

Contents

Introduction

The Australian Federal Police (AFP) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Law Enforcement (PJCLE) Inquiry into Combatting Crime as a Service.

The AFP is Australia's national policing agency and is part of the Home Affairs portfolio. The AFP has the jurisdiction to investigate Commonwealth (federal) crimes across Australia, as well as in the Australian Capital Territory (ACT). The AFP works with domestic and international partners across many types of crime, to address and mitigate these threats, and work together to defend and protect Australia and Australia's future from domestic and global security threats.

Organised Crime is a threat to Australia's domestic national security. Internationally, the nature of organised crime is evolving through:

1. Destabilising society through undermining social cohesion
    - Organised crime undermines and reduces trust in the rule of law
    - Organised crime is progressively driven by hybrid threats (criminal activities and tactics via criminal proxies)
2. Increased proliferation online
3. Accelerated use of technology
    - AI, encryption and other technologies – they all work as a catalyst for crime to improve efficiency, speed, reach, and sophistication.

Organised crime is highly agile to changes in the environment as they readily adapt to, adopt and exploit new technologies to their advantage and are on the lookout for new opportunities to take advantage of emerging technologies and changes in our behaviour. This evolving threat enables malicious actors to exploit vulnerabilities for financial and political gain, with the potential to impact national resilience, sovereignty, and prosperity.

The Crime as a Service model operates as a tiered structure, with criminal motivations ranging from immediate, low-skill profits, to sophisticated, long-term goals linked to eroding social cohesion and undermining Australia's democratic sovereignty. Less-experienced criminals can access readily available tools for quick financial returns, while state-level actors can use Crime as a Service for advanced, persistent campaigns aimed at intelligence gathering over extended periods.

Crime as a Service contradicts the Australian "fair go" principle, providing accessible tools for illicit activities and allowing individuals to profit from crime with reduced effort and risk. This undermines success being earned by legitimate individuals and business through merit and hard work. Criminal actors exploit digital vulnerabilities and human psychology through misinformation and disinformation campaigns, fuelling political polarisation, and undermining the community's faith in democratic institutions and disrupting social cohesion. Criminal actors can operate with a high degree of anonymity and a lower risk of punishment, circumventing the legal system that is meant to ensure fairness.

Crime as a Service

Crime as a Service refers to a model where individuals or organised crime groups hire services, tools, or the expertise from other criminals, often removing direct involvement from the facilitator, who may have links to foreign interests. As Australia's criminal and security environments have increasingly overlapped, Crime as a Service has demonstrated the willingness and ease with which offshore organised crime actors can undertake criminal acts that directly and indirectly impact Australia's domestic and national security.

The blurring of lines between state and non-state actors has created a complex and evolving threat landscape. Hybrid threat actors exploit criminal networks due to limited 'organic' resources for deniability and political influence or economic gain, while criminals benefit from protection, advanced tools and financial gain. Previously distinct operations are now merging, such as drug cartels using digital shadow economies for money laundering and state actors leveraging criminal groups to carry out attacks. Traditional organised crime groups, like drug cartels, are increasingly moving into the digital realm, adopting sophisticated, corporate-like structures with specialised roles for coders, project managers and negotiators. Organised crime now relies on the digital economy, including bulletproof hosting services and VPNs that provide the anonymity and security needed to evade law enforcement.

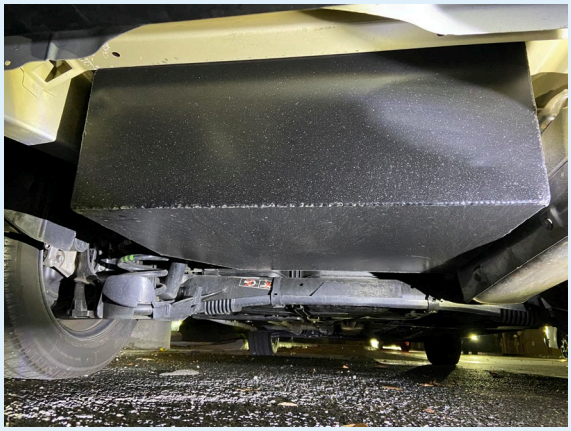
The proliferation of the Crime as a Service models is decentralising criminal capabilities, making attribution and disruption more difficult. This trend is accelerating and will require more agile, technology-enabled partnerships to enable successful disruption.

Vehicle Concealments

Criminal networks are increasingly adopting innovative, custom-built vehicle concealments to facilitate the movement of illicit drugs, weapons, and other illicit commodities or proceeds of crime with reduced detection risk. Syndicates commonly commission the professional installation of motorised, or RFID/remote-access compartments, paying upwards of $40,000 and utilising GPS tracking and coordinated logistics to monitor their assets in real time. These emerging tactics turn ordinary vehicles into purpose-built conveyances for organised crime, dramatically increasing concealment sophistication and operational resilience. Additionally, legislative gaps mean that the commissioning and installation of these hides can be completely legitimate, making them very difficult to police or prosecute.

The AFP Forensic Search and Imagery team, in collaboration with other key forensic disciplines, such as Forensic Intelligence, as well as the broader organisation, are enhancing capabilities to match this threat. Targeted intelligence-led stops, non-intrusive forensic imaging, bespoke scanning tools, and technical expertise are regularly deployed to locate and document remote-controlled or purpose-built hides to assist investigations. These concealments are often found empty, making it difficult to pursue further investigations. Legislative reform has begun in both the United Kingdom and United States to further combat this Crime as a Service and criminalise concealments such as vehicle hides in some circumstances. Pursuing similar legislative reform in Australia and expanding the work of Forensic Search and Imagery and other specialist capabilities will ensure greater support to joint operations between border agencies, AFP/ABF taskforces, and local policing jurisdictions to support the disruption and prosecution of organised crime and the logistics nodes that sustain these networks.

New South Wales – Hyundai iLoad – constructed hide in rear storage area.



Victoria – Peugeot Partner – Hydraulic hide under rear storage area.

Victoria – Toyota Camry – Constructed electronic hide between rear seats and boot.

The AFP has a unique role in identifying, deterring, disrupting and investigating organised crime groups impacting Australia, with a focus on creating maximum impact and strategic effect via strong international law enforcement agency relationships, industry partnerships, academia and through early intervention and disruption.

Cybercrime as a Service

Cybercrime as a Service is a business model in which cybercriminals offer cyber capabilities to customers. Would-be cybercriminals can buy access to networks, purchase tools to assist in evading security measures, as well as malware to deploy against victims and steal personal information.

Crime as a Service in the Community

Australia is facing a mix of multiple, significant, simultaneously elevated threats, driven by an uncertain international geopolitical environment and fuelled by domestic grievances. Australia is experiencing harm linked to reduced social cohesion, including an increased likelihood of politically motivated violence, an emotionally charged and intimidating protest environment, online radicalisation, and foiled extremist plots and terrorist attacks.

Organised crime involvement in adverse acts such as antisemitic attacks has almost certainly contributed to this environment, directly impacting Australia's national security through fostering discord and by undermining social cohesion.

Case Study – Operation HILFIELD

Operation HILFIELD is a Victorian Joint Counter Terrorism Team (JCTT) investigation into the arson attack on the Adass Israel Synagogue in Ripponlea, Victoria on 6 December 2024. The investigation was officially moved under the JCTT construct on 9 December 2024.

In August 2025, the Director-General of Security announced the attack against the synagogue was one of two antisemitic attacks in Australia directed by the Iranian Government. ASIO assessed there are links between some antisemitic incidents in Australia and commanders in Iran's Islamic Revolutionary Guard Corps, the IRGC. The AFP have intelligence consistent with this assessment. The arson attack has not been declared as a terrorist attack or an act of foreign interference.

The Victorian JCTT continues to investigate the matter as politically motivated violence and will consider appropriate offences based on the evidence available to prosecute offenders.

Crime as a Service is used by offshore organised crime actors to easily and rapidly approach and recruit local criminals or criminal groups to undertake a range of acts, including antisemitic violence. Previous overseas incidents have demonstrated how organised crime actors can organise attacks by leveraging criminal associations without the need for any shared ideological motivation by those undertaking the attacks.

Case Study – Operation KISSINGER

Operation KISSINGER is the investigation into a caravan found with explosives and antisemitic material in NSW in January 2025. The caravan was part of a fabricated terrorism plot orchestrated by organised criminals, both domestic and offshore, to cause fear for personal gain.

The investigation identified a number of people as part of the plot facilitated by taskings made on a secure platform investigators are collaborating with local and international law enforcement to bring all responsible parties to justice.

The plot had a significant negative impact on the Jewish community, causing fear and unwarranted suspicion toward other communities.

The AFP's Community Liaison teams and Senior Executive continue to have significant engagement with the Jewish community, other impacted communities, local law enforcement and government partners to support social cohesion efforts.

Youth

The AFP is seeing instances of criminal networks composed predominantly of pre-teen, adolescent and young adults, involved in a range of serious offences including cyber intrusions, cryptocurrency theft, sextortion, sadistic online exploitation and violence as a service. Criminal groups increasingly exploit young people as low-risk, disposable assets in Crime as a Service, with many of these young people not fully understanding the severity or consequences of their actions. Young people are often tasked with low-level activities such as becoming money mules or serving as couriers for items ordered with stolen data. Because there is limited direct contact with the facilitators, they may see themselves as simply following instructions, rather than participating in a crime.

Organised crime groups use social media and gaming platforms to target and groom young individuals, building trust by appealing to a young person's emotional needs for validation, belonging, or financial stability, blurring the lines between friendship and exploitation. Facilitators might present illegal tasks, like hacking or stealing data, as a game with increasing rewards, masking the serious criminal consequences. A lack of life experience and inability to fully assess risks makes young people particularly vulnerable to this type of exploitation.

Case Study – Operation DEDRIC

Operation DEDRIC is a foreign law enforcement referral into a 16-year-old young foreign national residing in Australia who facilitated Crime as a Service on behalf of a foreign organised crime network. The young person is alleged to have used the encrypted messaging platform Signal to solicit individuals to conduct murders and other crimes on behalf of the Foxtrot Network in Europe and the Middle East. They are alleged to have acted as a recruiter for the Foxtrot Network, seeking to enlist individuals to participate in criminal activity in exchange for compensation from the organisation, either in cash or cryptocurrency.

During the investigation, investigators monitored at least 29 posts made by the young person, in which he sought individuals willing to exchange cash for cryptocurrency, conduct contract

killings for substantial payments, handle explosives, and/or purchase weapons. In April 2025, the young person was arrested and charged with using telecommunications service to commit serious offences (conspiracy to murder), contrary to section 474.14(2) of the *Criminal Code 1995* (Cth).

The AFP is addressing this complex environment through a poly-criminal (offenders engaged in multiple crime types) operation, which was established in 2024, targeting the decentralised nature of these cybercriminal networks.

Internationally, the AFP has driven conversations with Five Eyes Law Enforcement Group (FELEG) partners in relation to this network and the operation has achieved major breakthroughs.

Beyond enforcement efforts, the operation has partnered with the Australian Centre to Counter Child Exploitation and prioritised victim welfare, identifying at-risk youth and engaging with families to provide support. Diversionary strategies have been employed to address the complex mental and physical health needs of victims.

The operation continues to evolve as a model of modern cybercrime enforcement, combining strategic coordination, international collaboration, and a strong victim-centred approach to dismantle the network and protect vulnerable individuals.

This cybercriminal network has highlighted a segment of cybercrime offenders who are youthful, inexperienced, anti-social, and sufficiently detached from the real world that they do not care or understand the reality of their criminal activities. Although they usually know their actions are wrong, and that people suffer, they are unsympathetic or unempathetic to others.

While the JPC3 Prevention team have worked to reduce youth involvement in cybercrime through prevention workshops like re_B00TCMP, there remains a challenge in bringing awareness to offenders and their families of the serious, and often horrific real- world consequences of cybercrime.

Physical and Online Environment

Crime as a Service is a commodity that exists in both the online and physical environment, where the tools and services to commit crimes are offered for sale. In Australia, this manifests through a supply chain for sophisticated online scams and ransomware attacks, drug trafficking, or the provision of services to carry out physical attacks such as targeted graffiti and arson.

Crime as a Service is increasingly segmented and fragmented. Different individuals or subgroups handle specific, discrete tasks, dividing the risk and responsibility, creating a chain of contractors and protecting higher level actors whilst exploiting those at the bottom. The low-level actor may be tasked with the relatively low-risk crime of stealing a vehicle, which is then passed through multiple recipients, before being used for its intended purpose. The person stealing the car knows only their small part of the operation and are not aware of the reasons for the theft or the identity of the final recipient. The fragmented nature of this process prevents participants from seeing the bigger picture and protects the facilitators. This process creates a cycle where vulnerable or unsuspecting individuals are drawn into a larger criminal enterprise.

Many cybercrimes also have real-world consequences, such as identity theft being used to commit fraud. The increasing reliance on digital and communications technologies creates new vulnerabilities and opportunities for cybercriminals. Combating crime as a service requires a multi-faceted approach that addresses both online and physical environments with strategies that focus on both prevention and response.

Under the remit of National Security Investigations, the AFP continues to focus efforts on Crime as a Service. AFP's National Security portfolio works closely with state and territory police to provide a nationally coordinated, consistent and intelligence-led response to security threats, and ensure all law enforcement and national security partners have the information needed to deliver the most effective and disruptive policing response.

Money Laundering

Money laundering is fundamentally a criminal service, as it is the process by which criminal groups can extract clean funds for their own usage. The criminal groups may pay to commission a standalone money laundering organisation to clean the proceeds, or the criminal groups may launder the funds themselves. The key challenges for law enforcement include untangling the web of processes used to 'clean' illicit wealth and intercepting the funds prior to the obfuscation of those funds. For criminal groups dealing in large quantities of cash, the vulnerability remains in entering the cash into the financial system without detection from regulatory agencies, the banking sector, or law enforcement.

Case Study

In February 2021, the AFP initiated an investigation into the activities of a suspected money laundering syndicate operating from a residence in the Sydney region, NSW. The residence was identified as a likely cash drop premises where illicit funds were stored after collection from organised crime groups, before being placed into the financial system.

It was determined that frequent, large quantities of cash would be dropped off at the premises by various cash runners and collected by an individual present at the residence. Upon receipt of the funds, the syndicate would structure the payments into a range of bank accounts controlled by the syndicate and then transfer the funds through a series of transactions to obscure the course.

As a result of search warrants executed by the AFP Anti-Money Laundering team, with support from partner agencies, approximately $3,500,000 in cash was identified, concealed in hidden compartments within the premises, using geomatic technology. One Australian citizen was arrested and subsequently convicted for dealing in proceeds of crime over $1,000,000. Proceeds of Crime Act (POCA) activity also resulted in the restraint of $33,684,355.12 (as of 16 June 2025).

This case study highlights the service that money laundering provides to organised criminal groups and the volume of cash the group can launder. It also demonstrates the enduring risk that money laundering poses to the Australian community, and the capability of the AFP and partner agencies in utilising new technology to continue to deter, disrupt and dismantle money laundering.

Money Mules

Money mules are individuals who are knowingly or unknowingly recruited by money laundering syndicates and then used by those syndicates to transfer stolen money in and out of their own accounts to make the funds appear legitimate to authorities.

Criminal networks will often target and recruit financially vulnerable individuals through fake job advertisements that promise easy money for minimal effort. Other common tactics include recruitment via online gaming platforms, social media, chat forums and online advertisements, or even face-to-face.

International students are particularly at risk due to aggravating factors such as financial vulnerability, looking for part-time or casual employment, and/or limited understanding of Australian laws with English being a second language.

Once recruited, these individuals – often unaware they are engaging in criminal activity – receive stolen funds into their personal bank accounts. They are then instructed to transfer the money to other accounts, typically overseas, and are allowed to keep a small portion as 'commission'.

Case Study – Operation WICKHAM

Operation WICKHAM investigated the systemic exploitation of predominantly Chinese students who were used to facilitate and establish private companies and open Australian business bank accounts.

The operation commenced in August 2022, when the United States Secret Service alerted the AFP-led Joint Policing Cybercrime Coordination Centre (JPC3) that millions of dollars in allegedly scammed funds were being transferred from the United States and other countries to Australian business bank accounts.

The investigation revealed that approximately $200 million had been stolen in the scam, and 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.

In total, 18 money mules were identified, with the majority being Chinese students, or recent arrivals into Australia on student visas. The AFP charged two of these students, with the remainder of the money mules not being charged due to insufficient evidence.

In addition to the two money mules, a further five parties were charged – responsible for controlling the money mules and those higher up in the money laundering syndicate.

One of the challenges faced in this matter, is the way money mules are recruited. Investigative matters among others, have identified marginalised groups of those under financial stress as the ones who are regularly targeted by money laundering syndicates. As such, a crucial component resulting from this operation has been through prevention messaging.

In 2024, JPC3 Prevention rolled out the #DontBeAMule campaign to raise awareness of the increasing trends that see university students recruited due to financial vulnerabilities. The campaign included marketing on university campuses and targeted campaign messaging at all Australian international airports and across online social media platforms.

Cryptocurrencies Facilitate Crime as a Service

The pseudonymity, low transaction fees and decentralised nature of cryptocurrency have been exploited by criminal syndicates to facilitate the movement of proceeds of crime. Crime as a service actors often advertise their preferred payment methods as cryptocurrency. They could openly publish their public wallet addresses for receiving payments then apply the following obfuscation techniques to launder the proceeds.

Decentralised Finance and Mixing Services

Decentralised Finance platforms facilitate trading and swapping cryptocurrencies without centralised exchange. The buyers and sellers are anonymous and there is no centralised KYC (know your customer) requirement. Some Decentralised Finance platforms have integrated functionality of breaking the link between the senders' wallet and receivers' wallet, known as a mixing service.

Non-Compliant Digital Exchange

In Australia, Crypto exchanges or Virtual Asset Service Providers (VASPs) are defined as financial institutions and are required by law to be registered with AUSTRAC. VASPs are also required to comply with the Anti-Money Laundering and Counter-Terrorism Financing Act (AML/CTF Act). However, overseas based VASPs are not bound by any regulations in Australia and do not readily respond to Australian law enforcement enquiries. Criminal syndicates, especially offshore based scam call centres, have been using overseas based VASPs to move scam victims' funds within seconds and convert to government issued currency (fiat currency) through those VASPs.

Crypto to Cash Desks/ATMs

Cryptocurrency ATMs (CATMs) act as on-ramps within the cryptocurrency ecosystem. They deal in cash, are often easy to use and find (especially in large cities), and rarely require registration beyond a phone number and at times an ID scan. Criminal syndicates leverage off this with their own fraud schemes, enabling CATMs to place cash and move funds anywhere in the world almost instantly.

CATMs have been identified to be used in various crime types including money laundering, terrorist financing, darknet market or child exploitation material purchases, drug trafficking, tax evasion, and fraud schemes.

Stablecoins

Use of stablecoins to move large sums of money in money laundering and scams is increasing. Cryptocurrencies can fluctuate by many percentage points in just a few days or hours. Stablecoins are a sub-set of cryptocurrencies that are pegged to the value of a stable asset. They offer a safe haven from the severe price volatility experienced by other cryptocurrencies. In order to run a profitable money laundering operation, a money launderer will want to reduce the risk of loss of value due to price fluctuations. Stablecoins reduce that risk.

Stablecoins are supported on newer blockchains such as TRON. Newer blockchains allow users to transfer funds across the world faster and at a lower cost than ever before. Money launderers can move funds from address to address many times for little cost in time and money.

Ransomware as a Service

Ransomware is malicious software that encrypts data and files when deployed onto a device or network. Cybercriminals use ransomware to disrupt operations and deny an organisation access to its systems or data, extorting payments from victims in exchange for the recovery of, and ability to re-access those systems and data. Ransomware is also an umbrella term to describe a demand for payment where data is stolen by cybercriminals but not encrypted.

The AFP and partners have observed a significant supply chain and professionalisation of the ransomware industry. Ransomware as a service has allowed criminals with relatively low technical capability to deploy sophisticated attacks against their victims. Criminal groups (and individuals) based around the world specialise in particular aspects of the ransomware business model and advertise their services to others.

The sectors with the highest number of reported ransomware incidents include:

- Education and training.
- Information, media and telecommunications.
- Professional, scientific and technical services.
- Government sector.
- Healthcare sector.

While ransomware continues to evolve rapidly, global law enforcement working collaboratively against dispersed cybercriminal service providers has achieved positive results in disrupting the threat.

However, there are current challenges for law enforcement. Ransomware is a relatively new crime of recent years, and significantly under-reported in Australia (and abroad). This is especially true for victims who opt to pay ransoms. Whilst a mandatory ransom reporting regime is now in place and will assist visibility of this crime type, it, does not obligate victims to cooperate with a police investigation. For corporate victims, dealing with the immediate cyber incident takes precedence over engagement with police, which can delay reporting and the provision of information.

As contracted incident response companies conduct their remediation processes, crucial evidence may be delayed or lost due to a lack of preservation of data and a lack of understanding as to what data can be accessed within certain timeframes, limiting law enforcement's ability to attribute those responsible.

Many ransomware offenders (and cyber criminals more broadly) utilise offshore IT infrastructure, often hosted in jurisdictions hostile to western law enforcement.

Furthermore, the use of encryption and other anonymising technologies create hurdles for law enforcement to be able to successfully identify and attribute these offenders.

Offenders involved in ransomware activities are also based offshore, frequently in jurisdictions unlikely to cooperate with Australian extradition.

Case Study – Operation ORCUS

Operation ORCUS is the AFP's ransomware taskforce representing Australia as part of the United Kingdom National Crime Agency-led international law enforcement joint investigation – Operation CRONOS.

Operation ORCUS is supported by the Joint Standing Operation between the AFP and Australian Signals Directorate (ASD) – Operation AQUILA, which leverages the complementary powers, capabilities and intelligence of the ASD and AFP to disrupt the most serious cyber threats facing Australia.

Operation ORCUS-JUNKERS is the AFP's strategic investigation into the LockBit Ransomware as a Service criminal group. The focus of the operation is to engage Australian based victims of LockBit ransomware to obtain indicators of compromise to identify the threat actors and their infrastructure.

In February 2024, a joint effort between AFP and United Kingdom-led Europol resulted in Operation CRONOS shutting down the LockBit primary platform, along with 34 servers across Australia, Netherlands, Germany, Finland, France, Switzerland, the United States and the United Kingdom.

- France's National Gendarmerie arrested two alleged LockBit actors in Poland and Ukraine, and a further three arrest warrants and five indictments were issued by French and United States law enforcement.
- More than 200 cryptocurrency accounts allegedly owned by the ransomware group were frozen by law enforcement, stripping the group of significant profits.

In May 2024, Australia, alongside the Five Eyes partners, the United Kingdom and United States, sanctioned Russian Dimitry Khoroshev after identifying him as a part of LockBit's senior leadership.

Domestically, since March 2024, the AFP has contacted 42 Australian-based LockBit victims.

Bulletproof Hosting

Bulletproof hosting (BPH) providers are a part of the Crime as a Service ecosystem and offer secure infrastructure to cybercriminals. Importantly, one BPH provider can directly enable hundreds of cybercriminals to target victims across the globe.

BPH providers lease cybercriminals a virtual and/or physical infrastructure that enables these malicious actors to store stolen data, host illicit content and run online criminal operations.

Major cybersecurity incidents affecting Australian organisations including disruptive ransomware attacks, theft of sensitive customer information and subsequent extortion, have been facilitated through criminals leveraging BPH providers.

Case Study – Cyber Sanctions (ZServers)

In February 2025, Australia, the United Kingdom, and the United States imposed targeted financial sanctions on the entity ZServers. Known as a BPH provider, this entity was a technical infrastructure service providing cybercriminals an online space to operate and host illicit content. ZServers systematically developed, provisioned, facilitated, and supported technologies enabling a range of cybercrimes, including ransomware activities conducted by affiliates of LockBit, BianLian, BlackSuit/Royal, ALPHV/Blackcat, and other ransomware groups.

Trilateral targeted financial sanctions, along with travel bans, were also placed on five Russian individuals for their roles in providing the infrastructure used to host and disseminate data that was stolen from Medibank Private in 2022. The individuals sanctioned were Aleksandr Bolshakov (ZServers' owner); Aleksandr Mishin and Ilya Sidorov (senior ZServers employees); and Dimitry Bolshakov and Igor Odintsov (ZServers employees).

The sanctions imposed make it a criminal offence punishable by 10 years' imprisonment for Australians and heavy fines for Australian businesses to provide assets to these individuals, use or deal with their assets, including through cryptocurrency or ransomware payments, and banned these individuals from entering Australia.

This marked the fourth cyber sanction Australia has supported, and the first directed at a criminal entity. Efforts were also made with industry to block ZServers' internet access and restrict their use of new financial services, which limited their ability to attract new customers.

Cyber sanctions work to disrupt and deter cybercrime and help protect Australians by exposing the identities of these cybercriminals and the malicious activities operating across jurisdictions. Sanctions increase the risk of detection for cybercriminals and malicious cyber actors by imposing serious costs and consequences to their actions.

The Australian Government's decision to sanction ZServers and associated cybercriminals was supported by the Department of Foreign Affairs and Trade. Operation AQUILA continues to deliver valuable intelligence and investigative cyber capabilities to the Australian Government in support of cyber sanctions.

International Role and Partnerships

Enablers of crime and their criminal infrastructure operate globally and are not bound by the location they reside in. Experience has shown global joint investigations have greater success in disrupting the criminal ecosystem. For long term disruption to be effective, Australian law enforcement must continue to collaborate with domestic and global partners to impact enablers targeting Australia. Additionally international collaboration enables further insights and intelligence sharing to establish clearer global linkages presenting further opportunities for collaboration on disruption of high value targets and networks.

Cyber threat actors are highly likely to collaborate or outsource elements of the offending to other cybercriminals, due to the diverse technical skills and capabilities required to undertake attacks. Typically, threat actors will specialise in one at times two particular skills, which they sell 'as-a-service'. Offering cybercrime capability as a service, lowers the risk thresholds for threat actors with minimal skill to undertake nefarious activities.

This dispersal of capability by many global cyber threat actors hinders law enforcement efforts by increasing anonymity and allowing offenders to collaborate, irrespective of geographical location.

Enablers, including their infrastructure, will almost certainly continue being dispersed globally, both in friendly and adverse jurisdictions. It remains difficult for a single law enforcement agency to work independently, with cybercriminal enablers often located in one jurisdiction, their infrastructure in a second and their victim in a third location.

The AFP has worked with its international policing partners for more than 50 years to combat crimes impacting Australia and our region, with personnel located in 35 countries around the world. The AFP's longstanding international partnerships provide important insights, within country, to the different approaches by other jurisdictions in policing and criminal law and justice issues.

Overseas, past incidents demonstrate how quickly organised crime entities can approach and recruit local criminal groups to undertake attacks and other criminal acts. In November 2022, antisemitic attacks in Germany were almost certainly orchestrated by an Iran-based organised crime actor under instruction of Iran's Islamic Revolutionary Guard Corps (IRGC).

Poorly understood links between these overseas groups and Australia reveals our exposure and potential susceptibility to Crime as a Service. However, differentiating instances of state/non-state actors using criminal proxies from conventional criminal acts orchestrated solely by criminal groups has posed a significant challenge for overseas law enforcement agencies.

Case Study - Sweden

In the European context, the definition applied to Crime as a Service focussed on young persons being actively targeted and recruited by organised crime groups and high value targets to commit acts of violence against rival gangs.

Sweden organised crime group related shootings have involved over 60 persons in the year to date up to 30 September 2025, with 33 being killed. Known perpetrators are predominately young persons, less than 15 years old, who are being recruited from youth facilities/homes and through social media platforms.

In response, Swedish authorities are actively monitoring the online/digital behaviours of young persons who are attracted to online applications and communication channels run by organised crime groups. Swedish authorities have had considerable success in the disruption space as a result of these efforts, preventing a number of serious crimes being committed in 2025.

Live Online Child Sexual Abuse

Live online child sexual abuse (LOCSA) is a child exploitation as a service that occurs across both the physical and online environment.

LOCSA facilitators provide a paid service for the abuse of children in real time, transmitted to a LOCSA consumer via a live stream. The majority of LOCSA facilities are located offshore.

Australia is known to be a demand side offender country for LOCSA offending in the Philippines and other Southeast Asian countries.

Philippine Internet Crimes against Children Centre

The AFP works with international partners to address the growth in LOCSA offending, establishing the Philippine Internet Crimes Against Children Centre (PICACC) which was officially opened on 27 February 2019. The centre is a joint effort of the Philippine National Police, the Philippine National Bureau of Investigation, the United Kingdom National Crime Agency, the International Justice Mission, and the AFP.

The centre's joint agency arrangement establishes collaborative cross-border efforts to protect children and provides a mechanism for foreign law enforcement to enhance the capability to investigate online sexual exploitation of children in the Philippines.

Under the National Strategy to Prevent and Respond to Child Sexual Abuse 2021-2023 (National Strategy), the AFP contributes to the Philippine law enforcement efforts to combat online child sexual abuse through dedicated child protection resources at the Manilla Post, exchanging criminal intelligence and information between Australia and the Philippines.

Virtual Global Taskforce

The Virtual Global Taskforce (VGT) is made up of 15 dedicated law enforcement agencies from around the world, working together to fight child sexual abuse.

The AFP, through the ACCCE, assumed the role of Chair of the VGT on 1 November 2024 for a three-year tenure.

In combatting child sexual exploitation, the VGT focuses on:

- Knowledge exchange
- Global influence and awareness raising
- Global threat scanning
- Seeking new opportunities to maximise impact
- Streamlining global lines of effort through international collaboration
- Operational and strategic workstreams

VGT members work together to deliver innovative, global strategies that address some of the biggest challenges facing law enforcement in tackling online child sexual abuse.

Priority areas for the VGT include LOCSA, under 18 offending, financial sextortion, Sadistic Online Exploitation, AI and End to End Encryption.

The segmentation and fragmentation of Crime as a Service enables these borderless crimes, with different actors in various countries specialising in discrete tasks – from content creation in one region to anonymous distribution and payment services in others – all shielded from the broader criminal enterprise. The VGT counters this by facilitating global cooperation, enabling law enforcement agencies to share intelligence, conduct joint operations and build capacity in forensics and investigation. This concerted international effort is essential in dismantling global supply chains that enable child sexual exploitation and other transnational crimes, directly confronting the challenges posed by Crime as a Service and its technological enablers.

What we need from Government and where to from here

Legislative Reform

There are opportunities to strengthen the legislative framework, which would further target-harden the Australian environment against organised crime groups and defend and protect Australia from the growing domestic and international threat. Unlike traditional organised crime structures, Crime as a Service operates through fluid, decentralised networks of collaboration, relying on opportunistic, project-based alliances among individuals with specialised skills, rather than on one, dominant leader. This makes Crime as a Service networks highly resilient and difficult for law enforcement to disrupt.

The proof required to establish the criminal association and organisation offences in the *Criminal Code Act 1995* (Cth) is extensive and complex, and the matters which the prosecution must establish beyond reasonable doubt to make out a criminal organisation offence can be challenging. Consideration could be given to strengthening the framework to assist AFP in targeting criminal organisations and their leadership.

Organised crime groups are continually evolving and are quick adaptors to new and emerging technology. The legislative framework has not kept pace with the modern digital environment. Reforms to the electronic surveillance framework would assist the AFP to prevent and defend against the organised crime threat in Australia. The laws need to be future proofed to accommodate advances in technology, meaning any new framework will need to be tech-neutral to ensure it is effective. A tech-neutral approach will support law enforcement to adapt to evolving threats and use modern capabilities.

The AFP has noted an increase in the manufacture, import and use of 3D printed firearms and gel-ball blasters. The weapons look and feel like conventional firearms, have the potential to cause serious harm, and can be manufactured cheaply and easily. Their realistic appearance and low cost make them attractive for criminal use, and they're increasingly being identified in serious criminal investigations. Consideration could be given to restrict the possession and sharing of blueprints for 3D printed firearms. There is also an opportunity to restrict the import (and by extension limit illicit trafficking) of gel-ball blasters and similar items, which would also support state and territory police efforts by limiting domestic availability of these items.

Simboxes are a key facilitator of large-scale cyber-enabled fraud, presenting a significant risk to the Australian public. These devices can send hundreds of thousands of malicious texts a day and present a domestic security threat. There is an opportunity to regulate the importation, possession and use of these devices. This would enable law enforcement to intervene earlier, rather than waiting until the devices are used in criminal activity.

Core police powers have not kept pace with new or emerging technology, processes and standards of information transmission. Enhancements to modernise core police powers would provide efficiencies for the AFP and increase capacity to defend against the evolving organised crime security threat. For example, ensuring the AFP has clear legislative basis to apply for its warrants and authorisations electronically, and providing 'notice to produce' powers so that AFP officers are not required to physically attend premises in person when obtaining information from non-suspect third parties, such as large financial institutions.

Addressing criminal activities at their source, rather than waiting for them to reach the reactive stage of law enforcement, can significantly reduce the need for constantly adding new legislation

and powers. This proactive approach places greater responsibility on industry and technology to harden targets, disrupt the underlying mechanisms of Crime as a Service, and prevent harm before it occurs. This creates downstream benefits for the community by increasing consumer safety, strengthening the financial system, and providing valuable intelligence to authorities. The AFP notes the recent announcements by Government to make amendments to the regulatory frameworks in the *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth), in this regard.