Australian Multicultural Acton Network Inc
32 Quandong Street, O'CONNOR ACT 2602
ABN: 40 172 914 431 Assn No: A06217

Mr Ravi Krishnamurthy JP
PRESIDENT

President.AMANACT@gmail.com
Mobile: 0404629700

---

06 October 2025

Submission to the Parliamentary Joint Committee on Law Enforcement

Inquiry into Combatting Crime as a Service
Prepared by: Ravi Krishnamurthy, President - Australian Multicultural Action Network (AMAN)
Date: October 2025

Introduction

I welcome the opportunity to contribute to this important inquiry into the challenges and opportunities for Australian law enforcement in combatting **Crime as a Service (CaaS)**. As President of the Australian Multicultural Action Network (AMAN) and an active participant in community and public policy discourse, I bring forward perspectives grounded in both grassroots community experiences and broader regulatory considerations.

The proliferation of Crime as a Service represents not only a law enforcement challenge but also a **national resilience issue**, impacting individuals, communities, and institutions across Australia. My submission seeks to highlight key concerns under the Committee's terms of reference and propose practical avenues for policy and enforcement improvement.

---

1. Nature and Impact of Technology-Driven Advancements on Criminal Methodologies

- **Crime-as-a-Service ecosystems** increasingly leverage darknet marketplaces, ransomware-as-a-service kits, and phishing toolkits available for purchase by low-skilled actors.
- **Cryptocurrencies** provide anonymity for money laundering, ransomware payments, and the trafficking of illicit goods. Decentralised finance (DeFi) further complicates traceability.
- Emerging technologies such as **generative AI** can enable sophisticated fraud, deepfake scams, and automated social engineering.
- These advancements lower the barriers to entry for criminal activities, enabling both organised crime syndicates and lone actors to operate with unprecedented reach.

---

2. Impact on Australians

- **Age:** Young Australians are disproportionately targeted through scams on gaming platforms and social media, while seniors are vulnerable to impersonation, investment, and romance fraud.
- **Gender:** Women, particularly in CALD communities, are more exposed to online exploitation, cyberstalking, and digital coercion.
- **Socio-economic status:** Lower-income households often lack the digital literacy and cyber-resilience measures to protect against fraud and identity theft.
- **Business type:** Small and medium-sized enterprises (SMEs) are especially vulnerable to ransomware and supply chain attacks, often lacking the resources to recover swiftly.

---

3. Challenges and Opportunities for Australian Law Enforcement

Challenges

- Jurisdictional complexity: Crimes originate offshore but impact Australians locally.
- Skills gap: Rapid technological innovation often outpaces law enforcement training and capacity.
- Evidence collection: Encryption and anonymisation tools limit digital forensics capabilities.

Opportunities

- Strengthening **public-private partnerships** with tech firms, banks, and telecom providers to disrupt CaaS supply chains.
- Investment in **specialist cybercrime taskforces** and continuous training.
- Leveraging **artificial intelligence and big data analytics** to proactively identify patterns in financial flows and digital behaviour.

---

4. Legislative, Regulatory and Policy Frameworks

- Current frameworks, including the **Criminal Code Act 1995** and **Anti-Money Laundering and Counter-Terrorism Financing Act 2006**, provide important foundations but may not be sufficiently agile to address CaaS innovation.
- There is a need for **adaptive legislation** that incorporates emerging technologies and keeps pace with international best practice.
- Data-sharing frameworks must balance **privacy and security**, enabling law enforcement and regulators to share intelligence without undermining civil liberties.

---

5. International Approaches

- The **European Union's Digital Services Act** demonstrates how regulatory obligations can compel online platforms to mitigate illicit use.
- The **FBI and Europol Joint Cybercrime Taskforces** highlight the value of transnational coordination.
- Australia can strengthen its role by engaging more actively in multilateral cyber agreements, and by embedding **liaison officers** in global law enforcement hubs to ensure intelligence flows seamlessly.

Recommendations

1. **Establish a National CaaS Threat Coordination Centre** to consolidate law enforcement, regulatory, and industry expertise.
2. **Mandate stronger obligations for cryptocurrency exchanges** operating in Australia, including enhanced KYC (Know Your Customer) and transaction monitoring.
3. **Expand digital literacy programs** targeting seniors, youth, and SMEs, with particular focus on CALD communities.

4. **Strengthen international law enforcement cooperation** through secondments, treaties, and shared training platforms.
5. **Legislate adaptive regulatory mechanisms** that can evolve alongside emerging technologies, rather than relying on static legislative reviews.

Conclusion

Crime as a Service poses a complex and evolving threat to Australia's security, economy, and community wellbeing. By adopting a **holistic approach**—combining legislative reform, law enforcement innovation, community education, and international collaboration—Australia can build resilience against this digital menace.

I commend the Committee for undertaking this timely inquiry and trust that these perspectives will contribute to strengthening our nation's response.

Respectfully submitted,

Ravi Krishnamurthy