Crime as a Service Challenges and Opportunities for Australia

Introduction

Crime as a Service (CaaS) marks a transformative shift in the landscape of global and transnational crime, rivalling the impact of the industrialisation of the drug trade. By enabling non-technical individuals to purchase or rent the tools, infrastructure, and expertise needed for cyber and financial crimes, CaaS has democratised digital criminality.

Today, sophisticated attacks such as ransomware and data theft can be executed with minimal technical knowledge, thanks to the proliferation of illicit online marketplaces. The Australian Institute of Criminology describes this as the "commodification of criminal capability," a development that has dramatically increased both the volume and complexity of cyber-enabled crimes.

The Broader Impact of CaaS

CaaS is not just a technical or legal issue—it is also a philosophical and political challenge. It tests the ability of democratic societies to balance openness and privacy with the need for security, especially as adversaries exploit these very qualities. Australia now faces a critical opportunity: to craft a response that is innovative, evidence-based, and respectful of citizens' rights. Parliament must lead by establishing frameworks, institutions, and partnerships that operationalise this balance.

Building Social Resilience

Effective enforcement alone is insufficient. Social resilience—at both individual and organisational levels—is essential for protection against cybercrime. Prevention, awareness, and victim support services must form the foundation of Australia's response. Public education campaigns should be ongoing and tailored to different age groups and cultural backgrounds to maximise their impact. Mandatory incident reporting and a trusted national cybercrime reporting portal would enhance visibility and coordination, empowering both government and industry with the data needed for effective action.

Regulatory and Legislative Reform

Australia's regulatory bodies should encourage or require "secure-by-design" principles across fintech, telecommunications, hardware, and software sectors, as these industries form the backbone of criminal infrastructure. Law enforcement needs legislative clarity, bipartisan political support, sustained resources, and a culture of technological adaptability. A national CaaS Disruption Strategy could unify intelligence efforts, target high-impact threats, and foster collaboration across federal and state levels.

International cooperation is also vital. The Federal Government should prioritise fast-tracking data-sharing agreements that protect data sovereignty while enabling near real-time exchange of digital evidence. Legal frameworks must criminalise the provision of unauthorised cyber-security services, aligning with global standards to balance innovation and accountability. Investment in workforce development is crucial, with incentives to attract and retain cyber specialists in investigations, prosecutions, and forensics.

Learning from International Models

Australia can draw lessons from international approaches. The European Union's Digital Services Act and AI Act require online service providers to remove illegal content and hold suppliers accountable for their algorithms. In the United States, the Department of Justice targets the infrastructure of cybercrime through coordinated takedown operations. The UK's National Crime Agency and Europol's European Cybercrime Centre serve as regional hubs, connecting intelligence with operational response. These examples show that success depends not just on stronger capabilities, but on coherent governance and real-time alignment among government, industry, and international partners.

Current Gaps and Opportunities

Australia's current legislative and regulatory structures are evolving but remain fragmented. The Telecommunications and Other Legislation Amendment Act 2018 granted agencies decryption powers, but their use has been slow and controversial. Ongoing reforms to electronic surveillance laws present an opportunity to clarify warrant thresholds and update processes while safeguarding civil rights. Financial regulation of digital currency exchanges has improved transparency, but significant gaps remain, particularly with decentralized finance and unregistered offshore providers.

Critically, Australia lacks specific laws to criminalise the operation and facilitation of CaaS platforms, forcing prosecutors to rely on outdated conspiracy and computer misuse provisions.

Innovative Responses and Partnerships

Despite these challenges, there are positive developments. Advances in blockchain analytics now allow investigators to trace illicit money flows. Collaborative partnerships, such as those enabled by CI-ISAC Australia and AUSTRAC's Fintel Alliance, facilitate intelligence sharing and generate leads that no single organisation could produce alone. High-profile operations, like the AFP's infiltration of encrypted communication platforms, demonstrate the value of combining technical expertise, legal authority, and international cooperation.

Ongoing Challenges

However, technology continues to evolve faster than government agencies can adapt. Criminal tactics and technologies outpace procurement and training cycles, and jurisdictional complexity—both interstate and international—complicates enforcement. Most CaaS platforms operate overseas, often beyond the reach of Australian law.

Traditional law enforcement cooperation mechanisms are too slow for the rapid pace of modern cybercrime. The rise of end-to-end encryption and zero-knowledge systems further limits the effectiveness of lawful interception powers, making it increasingly difficult for police to access even metadata.

Vulnerabilities and Victimisation

Australians of all ages are vulnerable to cyber-enabled harms, though impacts vary. Younger, digitally native individuals are more likely to fall victim to cryptocurrency scams and social media fraud, while older Australians are disproportionately targeted by romance scams and identity theft. Socio-

economic disadvantage exacerbates these harms, with low-income and digitally excluded groups suffering losses they cannot recover. International students, particularly those from non-English speaking backgrounds, are targeted by scams exploiting language barriers and fears of deportation. Small and medium businesses without dedicated security staff are easy targets for ransomware and business email compromise attacks. Ultimately, these crimes erode trust in digital infrastructure and law enforcement, fostering fear and anxiety about online safety.

The Role of Technology in CaaS

CaaS thrives on technologies that enable anonymity, scalability, and automation. Cryptocurrencies and privacy tools, originally designed for legitimate innovation, now facilitate transnational illicit networks. Ransomware groups launder profits through mixers and privacy coins, while cloud hosting and encrypted communications provide secure environments for coordination. Generative AI is increasingly used to craft convincing phishing campaigns and deepfakes. This convergence of technologies has given rise to "hyper-crime"—criminality accelerated by artificial intelligence, not just digitised by human actors.

Conclusion and Recommendations

Australia faces significant challenges in combating CaaS, but also has unique opportunities to lead with innovative, rights-respecting solutions. Key recommendations include:

- Strengthening legislative frameworks to specifically target CaaS platforms and unauthorised cyber-security services.
- Enhancing public education and social resilience through sustained, targeted awareness campaigns.
- Fostering public-private and international partnerships for intelligence sharing and coordinated response.
- Investing in workforce development to close the skills gap in cyber investigations and forensics.
- Promoting secure-by-design principles across critical industries.
- Accelerating international data-sharing agreements that protect privacy while enabling rapid evidence exchange.

By aligning government, industry, and international partners around shared goals, Australia can build a robust, adaptive response to the evolving threat of Crime as a Service.

CI-ISAC Australia
8th October 2025

info@ci-isac.org.au

https://www.ci-isac.org.au