accenture

ACCENTURE SUBMISSION

Parliamentary Joint Committee on Law Enforcement

Inquiry into the Challenges and Opportunities for Australian Law Enforcement in Combatting Crime as a Service

Pursuant to subsection 7(1) of the *Parliamentary Joint Committee on Law Enforcement Act 2010* (Cth)

Introduction

Technology-driven criminal enterprises are evolving and scaling faster than ever before. Crime as a Service (CaaS) represents a growing and complex threat in which illicit tools, platforms and expertise are made available for purchase or hire, enabling criminal groups to outsource activities that once required technical sophistication or physical coordination. Unlike traditional organised crime, these networks are decentralised, scalable and increasingly anonymous making them harder to track and disrupt.

Australia's law enforcement and intelligence communities are under significant pressure to respond to these rapidly shifting threats. However, a consistent concern across operational policing partners is that the pace of government-led innovation and procurement, coupled with underfunding and governance bottlenecks has left law enforcement behind. Criminals face few barriers to access advanced tools via the dark web or rented infrastructure, while agencies must navigate long lead times, internal competition for limited resources and a governance model not optimised for technological agility.

NCIS presents a powerful opportunity to become the national vehicle for embedding automation and artificial intelligence (AI) in real-time crime detection and disruption, particularly for emerging threats such as CaaS.

Integrating automated AI scanning tools directly within the NCIS environment would enable law enforcement to detect hallmark indicators of CaaS operations, such as repeat use of digital identities or handles, common modus operandi involving money mule recruitment, or recurring patterns across cyber-enabled crimes.

In the future, AI agents leveraging Agentification AI could autonomously monitor open and closed sources, flag suspicious behaviours and cross-reference entities across jurisdictions, significantly accelerating the intelligence cycle. These bots would operate within NCIS parameters to ensure both lawful use and data security, alerting human analysts to high-probability threats in real-time and reducing investigative burden.

The nature and impact of technology-driven advancements on criminal methodologies and activities, including the use of cryptocurrencies

The digital landscape has dramatically changed the way crime is conceived, executed and monetised. CaaS enables individuals or groups to carry out complex cyberattacks without owning the underlying infrastructure or even possessing the requisite skills. With the growing commoditisation of malware, ransomware-as-a-service, deepfake tools and cryptocurrency laundering services, virtually anyone can now access capabilities once limited to nation-state actors.

The democratisation of crime is being rapidly accelerated by the accessibility of cloud infrastructure, which can now be rented on an hourly basis. This enables individuals and small groups to scale malicious operations to levels that rival those of nation-states or large enterprises. The emergence of AI introduces an additional layer of complexity facilitating automation, sophisticated social engineering and the generation of synthetic identities at scale. Criminal actors are already exploiting AI to create highly adaptable, targeted and evasive attack models. The growing 'steal now, decrypt later' threat further

complicates long-term national cybersecurity strategies, underscoring the need for forward-looking investment and policy co-ordination.

Encrypted messaging platforms, have further enabled secure and anonymous coordination of transnational criminal activities. In parallel, the rise of Disinformation-as-a-Service (DaaS) is facilitating highly tailored manipulation campaigns, including fabricated terrorism incidents designed to instil fear, destabilise communities, or exert political influence.

The criminal use of large language models (LLMs) and AI tools is also challenging existing legal and regulatory frameworks, particularly in areas such as theft, intellectual property and content ownership where AI-generated outputs may be based on proprietary or copyrighted data. Additionally, bot farms and automated systems are increasingly being deployed both to carry out large-scale cyberattacks and to amplify disinformation across social media and other digital platforms.

Cryptocurrencies continue to play a central role in concealing illicit financial flows. However, the ability of law enforcement to effectively track and disrupt these transactions is increasingly constrained by the high cost and complexity of commercial crypto-tracking software, often placing such tools beyond the reach of standard policing budgets. At the same time, criminal actors are rapidly adopting and discarding digital wallets, rendering manual tracking approaches largely ineffective.

This creates a growing mismatch between the speed, scale and sophistication of criminal activity and the limited responsiveness of current policing capabilities. To close this gap, law enforcement must shift from reactive approaches toward proactive, intelligence-led and technology-augmented operations.

We recognise that police forces operate under significant budgetary and resourcing constraints. For example, the cost of commercial crypto-tracking software licences remains a major barrier to widespread adoption and operational effectiveness.

Accenture would welcome opportunities to collaborate on next-generation solutions, including the application of Agentification AI. This technology has the potential to be a transformational ‘game changer’ in identifying, tracking, and disrupting criminal behaviour, particularly in environments where traditional software-as-a-service and rules-based systems are no longer sufficient to deal with the scale, sophistication and agility of modern criminal networks.

The Government could enable the development of a suite of intelligent autonomous bots designed to continuously scan, correlate and surface high-risk patterns and behaviours associated with CaaS. These automated detection agents could operate within the federated NCIS environment leveraging integrated data from multiple jurisdictions and Commonwealth sources to proactively detect threats and generate real-time intelligence leads.

Key use cases include:

- Cyber Threat Signature Correlation: Automated agents can monitor for simultaneous scans and intrusion attempts using identical malware payloads, exploits, or techniques across multiple geographies indicating a co-ordinated or

syndicated cyber campaign. These signatures can be automatically flagged and linked to known threat actors or emerging CaaS offerings.

- Dark Web Intelligence Monitoring: Bots can monitor high-risk forums and marketplaces on the dark web for emerging CaaS services (for example, ransomware-as-a-service, credential dumps, exploit kits), triggering alerts when new offerings appear or when known handles resurface. This enables law enforcement to task covert online operatives with precision and speed.
- Cross-Jurisdictional MO Pattern Matching: Machine learning algorithms can identify recurring patterns in criminal modus operandi such as logistics fraud, identity theft scams, or business email compromise that appear across states or regions but may otherwise be treated in isolation.
- Handle/Pseudonym Reuse Detection: AI agents can detect when similar or identical pseudonyms are used across multiple cases or platforms, helping to establish links between seemingly unrelated incidents or digital personas operating in different jurisdictions.
- Gang and Syndicate Activity Mapping: Bots can detect repeated references to known gangs or organised criminal groups in incident data, financial transactions, or communications metadata, indicating patterns of facilitation, recruitment or transnational operations.
- Money Mule Identification: AI can analyse financial transaction patterns and behavioural indicators to detect likely money mule activity, particularly when accounts are being used to rapidly funnel or distribute funds consistent with CaaS operations.
- Phishing and Social Engineering Campaign Tracking: Bots can detect when identical phishing kits or lures are deployed en masse, allowing investigators to trace source infrastructure, identify reused assets and disrupt operations before widespread harm occurs.
- Synthetic Identity Detection: Using behavioural biometrics and identity verification signals, automated systems can detect synthetic identities being used to open accounts, register services, or receive illicit funds, often a core enabler of CaaS operations.
- Supply Chain Compromise Monitoring: Bots can be used to monitor breaches and compromises of critical suppliers or vendors that may indicate a broader strategic intrusion campaign, especially where CaaS actors use compromised services as entry points.
- Real-Time Takedown Co-ordination: AI can help co-ordinate rapid disruption efforts across multiple jurisdictions when CaaS infrastructure (for example, malware C2 servers or carding sites) is detected, reducing response time and improving impact.

By embedding these intelligent detection capabilities into NCIS, law enforcement agencies can shift from reactive investigation to proactive disruption, with AI agents serving as force multipliers for analysts, intelligence officers and frontline responders.

The impact of these technology-driven crimes on Australians, including age, gender, socio-economic status and business type

Technology-enabled crime is affecting a growing number of Australians, cutting across all demographics and economic sectors. Vulnerable populations, including the elderly, youth and individuals with limited digital literacy, are increasingly being targeted by scams, ransomware, phishing and identity theft. Women face unique risks in online abuse, particularly through social engineering and impersonation on social platforms.

Small and medium enterprises (SMEs) are particularly exposed due to limited investment in cybersecurity, making them common targets for ransomware, invoice scams and business email compromise. Larger corporations may recover from such attacks, but SMEs often lack the resilience to survive the fallout. These impacts have ripple effects on employment, supply chains and consumer confidence.

A major obstacle to effective prevention and response is that cybercrime remains significantly underreported. This underreporting renders much of the threat landscape invisible to key agencies. It limits the ability to learn from incidents, proactively defend against new tactics and strengthen community and business resilience. Notably, those most at risk, such as older Australians, small businesses and lower socio-economic groups are often the least equipped to protect themselves or recover from cyber incidents.

Operational police partners report being under increasing pressure to deliver enhanced capabilities with shrinking resources. Some have responded by innovating with limited means. For example, using non-commissioned individuals to create and manage undercover digital personas for infiltrating criminal groups. These individuals bring unique perspectives, and skill sets not typically found in traditional law enforcement. However, their effectiveness is limited by constraints on funding, governance and access to advanced technology. AI could radically enhance this capability, enabling automated creation and maintenance of online identities, reducing the operational burden and expanding reach into digital criminal networks.

The burden of crime does not fall evenly. The impact is amplified among disadvantaged communities, both in terms of victimisation and in access to justice and recovery mechanisms. Law enforcement must have the tools and mandate to detect, deter and disrupt cyber-enabled crime across all levels of society.

Challenges and opportunities for Australian law enforcement in combatting evolving criminal methodologies

Despite the establishment IT and professional services panels to improve the ability to go to market and onboard new tools, services and partners at speed, Australian law enforcement faces significant challenges in responding to rapidly evolving criminal methodologies, particularly those enabled by digital technologies and the globalisation of CaaS. While criminals can gain access to illicit tools and services within minutes via the dark web, agencies often navigate lengthy procurement cycles to obtain equivalent defensive capabilities.

Oversight mechanisms, although essential for accountability, often create delays in accessing systems and materials, hampering operational responsiveness in situations where intelligence must be acted upon quickly. Funding shortfalls, internal competition

for limited resources and the absence of a unified innovation strategy across jurisdictions have created a fragmented capability base.

Moreover, one of the most significant structural weaknesses is the lack of interoperability and trust between agencies. The absence of shared data standards and systems results in siloed intelligence, duplicated efforts and missed opportunities to disrupt criminal activity. Persistent mistrust both between agency staff and government, and across federal and state jurisdictions further undermines collaboration. Without unified leadership and a clear strategic vision, Australia's response to CaaS will remain fragmented, reactive and vulnerable.

Despite these challenges, AI offers major opportunities to augment intelligence analysts by identifying patterns at scale and generating leads that would otherwise remain buried. AI has the potential to reduce administrative burdens, accelerate trend detection and support predictive threat modelling, allowing analysts to focus more on decision-making rather than data wrangling.

Authorities should consider establishing a register of user 'handles' and employing AI to help identify offenders across platforms. It is understood that investigations into CaaS offences are often stalled due to difficulties in identifying offenders. Furthermore, while efforts rightly prioritise serious offenders and networks, there should also be consideration given to proactively alerting lower-level networks and individuals to the fact that authorities are aware of their activities. Automated letters could be sent regularly to such individuals, informing them that they are being monitored, which has been proven to help reduce opportunistic crime.

In cases involving financial-related cybercrimes, authorities should consider adopting an 'AMBER Alert'-style notification process to alert financial institutions of potential fraud. Similar to disaster notifications, this system would enable institutions to act quickly and collaboratively in response to criminal incidents related to CaaS. This real-time alert mechanism would improve the agility and effectiveness of responses to financial cybercrime, supporting a more proactive approach.

Australia has a strong foundation in law enforcement and intelligence, but current approaches are too slow, fragmented and constrained by outdated structures to effectively combat rapidly evolving digital criminal methodologies. To remain competitive and effective, Australian agencies must streamline technology adoption, invest in AI and automation tools, foster trust and interoperability across jurisdictions, embrace proactive intelligence-led disruption strategies and deepen collaboration with the private sector. Such reforms are essential to equip Australian law enforcement to meet the challenges of the digital age strategically, operationally and technologically.

Whether existing legislative, regulatory and policy frameworks are fit for purpose

The traditional legislative and regulatory frameworks are struggling to keep pace with the speed, structure and scale of digital crime. While these frameworks are designed to ensure ethical and accountable operations, they often impede rapid innovation. Governments tend to focus on protection rather than resilience and recovery, while agencies must spend more time on compliance than on innovation.

Criminal actors face none of these constraints. They operate with impunity across borders, using temporary infrastructure, concealed identities and decentralised collaboration. Agencies by contrast, are hampered by policy and legislative delays and by a culture that does not adequately reward risk-taking or innovation.

Data governance remains a particular concern. Agencies are often reticent to share data beyond traditional boundaries due to fears of breaching data sovereignty rules. Yet ironically, the biggest threat to data security remains the trusted insider, whether through negligence or malicious intent. There is an opportunity for agencies to deploy AI-driven systems to track data exfiltration, monitor its presence on the dark web and proactively respond to breaches.

Policy development must shift from a purely defensive posture to one that also prioritises strategic agility, cross-sector resilience and offensive capability development. This includes regulatory support for ethical AI deployment, standardised minimum cybersecurity frameworks for SMEs and streamlined procurement pathways for critical technology.

International approaches to combatting Crime as a Service

Globally, law enforcement agencies are adopting more agile and innovative strategies to counter the rising threat of CaaS. In jurisdictions across Europe and North America, AI-powered tools are being deployed to proactively monitor the dark web for indicators of criminal activity. These systems use machine learning and natural language processing to scan illicit marketplaces and forums, enabling near real-time detection of emerging threats, actors and illegal transactions.

Cybercrime supply chains frequently originate in Eastern Europe and the Indo-Pacific, highlighting the need for Australia to develop a regional lens rather than relying solely on Euro-American models. The case of Myanmar, where organised criminal groups have formed alliances with armed factions, exemplifies the intersection of criminal enterprise and geopolitical instability, further complicating law enforcement and intelligence responses.

The global availability of illicit services, including ransomware deployment, botnet rentals and forged documentation, demonstrates how crime is now offered ‘as a service’, operating across borders with minimal friction. Effectively disrupting these networks will require Australia to deepen engagement with international partners, including multilateral policing forums, regional cyber coordination centres and diplomatic initiatives. Cross-border collaboration, harmonised cybercrime definitions and joint intelligence efforts are essential to dismantle these transnational ecosystems.

Real-time public-private collaboration frameworks are becoming standard practice internationally. In the United States, for example, alert systems now notify financial institutions of active cyber threats within minutes, enabling rapid preventative action. By contrast, Australia remains relatively disconnected from the global technology supply chain and is often viewed by major technology providers as a lower-priority partner, despite public official statements promoting collaboration. This reputational gap, limits Australia’s access to emerging tools, pilots and early-stage innovation pipelines.

Australia must also address its strategic lag in preparing for quantum-era threats. While countries such as the United States and China are already investing heavily in quantum-resilient encryption and post-quantum planning, Australian agencies remain under-resourced and under-informed about the long-term implications. Without targeted capability-building, Australia risks falling further behind in protecting its digital infrastructure against next-generation threats.

Globally, law enforcement and intelligence agencies are moving toward faster, more integrated and more transparent partnerships. To remain relevant and effective, Australian agencies will need to keep pace, not only in technology adoption but also in leadership, mindset and operational culture.

Conclusion

The accelerating pace and sophistication of technology-driven crime present a formidable challenge to Australia's law enforcement and intelligence agencies. CaaS and related cyber-enabled criminal methodologies have transformed the threat landscape, enabling decentralised, scalable and increasingly anonymous operations that outpace traditional policing capabilities. Despite a solid foundation in law enforcement, current Australian approaches are hindered by slow procurement processes, fragmented capabilities, limited interoperability and outdated governance models that are ill-suited to the demands of the digital age.

To effectively counter these evolving threats, Australian agencies must embrace innovation, agility and collaboration at all levels, across jurisdictions, with industry partners and within international frameworks. Leveraging emerging technologies such as AI and automation offers a critical opportunity to enhance intelligence-led operations, reduce administrative burden and proactively disrupt criminal networks. Moreover, strategic investment and reform in legislative, regulatory and operational frameworks are essential to keep pace with the scale and complexity of digital crime, protect Australians across all demographics and safeguard the nation's economic and security interests.

Recommendations

1. *STREAMLINE PROCUREMENT AND INNOVATION PATHWAYS*
   Reform governance and procurement processes within law enforcement to significantly reduce lead times for adopting new technologies. Enable pilot programs and agile procurement models to ensure faster deployment of critical capabilities.
2. *INVEST IN AI AND AUTOMATION TECHNOLOGIES*
   Prioritise funding and partnerships to develop and deploy AI-powered tools, to operate within the federated NCIS environment, that enhance pattern recognition, offender identification, predictive threat modelling and automated monitoring of digital criminal ecosystems. Explore opportunities to leverage Agentification AI to transform crypto-tracking and cybercrime investigations.
3. *ENHANCE INTEROPERABILITY AND DATA SHARING*
   Establish national standards for data sharing, common protocols and interoperable systems across federal, state and territory agencies to reduce silos and duplication.

Foster trust through transparent governance frameworks and collaborative leadership structures.

4. *ADOPT PROACTIVE AND INTELLIGENCE-LED DISRUPTION STRATEGIES*
   Implement programs that alert lower-tier offenders to monitoring efforts and develop mechanisms such as 'AMBER Alert'-style notifications for financial institutions to rapidly respond to cyber fraud incidents. Promote a culture of proactive disruption rather than reactive enforcement.
5. *MODERNISE LEGISLATIVE AND REGULATORY FRAMEWORKS*
   Review and update existing laws and policies to support rapid innovation, ethical AI deployment and cross-sector resilience. Address data governance challenges by balancing privacy and sovereignty concerns with the need for timely intelligence sharing and breach response.
6. *STRENGTHEN INTERNATIONAL COLLABORATION AND PARTNERSHIPS*
   Enhance Australia's engagement with global law enforcement and industry partners to access cutting-edge tools, share intelligence and participate in joint initiatives. Address reputational barriers that limit Australia's inclusion in global technology supply chains and innovation programs.
7. *PREPARE FOR QUANTUM-ERA CYBERSECURITY THREATS*
   Invest strategically in building quantum preparedness capabilities, including research, threat modelling and defensive measures to protect critical digital infrastructure from emerging quantum decryption risks.

By embracing these recommendations, Australia can develop a more agile, technologically sophisticated and unified law enforcement framework, one that is well-equipped to confront the complex and rapidly evolving challenges of technology-driven crime. Accenture looks forward to continuing engagement with the Committee to support the implementation of these initiatives and contribute to a more secure, intelligent and resilient future for Australia's law enforcement community.