AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

SUBMISSION

PJCLE Inquiry into Combatting Crime as a Service

INTRODUCTION

The Australian Criminal Intelligence Commission (ACIC) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Law Enforcement inquiry into Combatting Crime as a Service. (U)

The ACIC's purpose is to protect Australia from serious criminal threats by collecting, assessing and disseminating intelligence and policing information. Critically, the agency supports whole of government decision-making across operational practice, policy, regulatory and legislative environments. (U)

The ACIC:

- provides unique, actionable and insightful criminal intelligence and advice to government on serious and organised crime (SOC) – including where it has a transnational dimension – through collecting and analysing information and data about complex offending patterns and criminal business models, criminal groups, networks and individuals across multiple crime vectors
- undertakes special ACIC investigations and operations as authorised by the ACIC Board for purposes including identifying vulnerabilities in particular systems and collecting and disseminating intelligence – as well as evidence of particular offences – to facilitate enforcement, prevention, disruption and regulation activities
- provides national policing information systems and services to law enforcement and intelligence partners to keep them and the Australian community safe
- delivers background checking services to support employment or entitlement decisions and to maintain community safety. (U)

OPERATING CONTEXT

Today's SOC networks are more sophisticated than ever before. They leverage global connections and infrastructure to engage in criminal activities that impact Australia's national security, safety and prosperity. They employ sophisticated technology and tradecraft to enable and expand their criminal pursuits. More than ever, they are also primarily based offshore, which poses additional operational challenges for intelligence and law enforcement agencies. (U)

SOC networks are borderless, decentralised, digitally enabled and increasingly embedded within legitimate systems. They operate with the agility and sophistication of multinational businesses and exploit infrastructure, encrypted communications and the cyber domain to expand their reach, diversify criminal activities and evade intelligence and law enforcement detection. (U)

Rival crime groups now collaborate across hierarchical, familial and ethnic lines. Previously isolated and competing SOC networks, now collaborate in joint ventures to leverage each other's resources and specialist capabilities to expand illicit markets and maximise profits. Further, SOC networks can operate as loosely connected networks of individuals and service providers – rather than traditional hierarchical organisations – which can make their identification challenging. This evolving environment poses significant risks to Australia's national security, safety and prosperity. (O)

The Australian Institute of Criminology estimated SOC cost Australia up to $68.7 billion in 2022-23 – equivalent to 2.9% of Australia's gross domestic product. These are significant profits in the hands of criminals at the expense of the Australian community and tax payer. (U)

With SOC threats becoming increasingly complex, adaptive and transnational, the ACIC must operate at a pace that matches the threat environment. This requires an intelligence-led posture – leveraging advanced collection, analysis and assessment capabilities to illuminate hidden and dynamic criminal ecosystems. This also informs operational and policy decision-making to harden the environment against SOC exploitation and to keep Australia and Australians safe. (U)

EMERGENCE OF CRIME AS A SERVICE

SOC networks seek to systematically exploit vulnerabilities in Australian and international systems for profit. They also increasingly rely on insiders with privileged accesses and professional facilitators with exploitable skills to circumvent detection and disruption efforts and enable their activities. Professional facilitators are individuals who possess specialist qualifications and knowledge who are used – wittingly or unwittingly – to facilitate the misuse of professional services in support of criminal activities. These include – but are not limited to – lawyers, accountants, registered migration agents, real estate agents and customs brokers. (O)

Further, but separate to the use of professional facilitators, 'crime as a service' is a business model within the criminal economy. It involves the specialisation, professionalisation, marketing and solicitation of criminal services. Rather than a single distinct criminal network managing all stages of an illicit operation, 'crime as a service' enables individuals or groups to specialise in specific functions and market these services to others. This model enables a range of actors to purchase criminal capabilities by tasking criminals who offer illicit services to support their specific objectives. It enables SOC networks with limited expertise to expand and diversify their criminal activities. Critically, it lowers the barriers to entry, enabling individual actors – not just established SOC groups – to engage in complex or large-scale criminal activity. (O)

Criminals outsourcing or contracting others to commit crimes is not a new phenomenon – the 'crime as a service' model supports offending across a range of activities. In the digital age, 'crime as a service' provides the opportunity for a new generation of digital natives to engage in serious criminal activities. The 'crime as a service' model allows SOC networks to gain resources and optimise their profits, while developing mutually beneficial partnerships with other SOC networks. The use of 'crime as a service' can also impede the discovery of threats and make it difficult to identify offenders. SOC networks are willing to adopt any new technology that is readily available, accessible, cost-effective and achieves the desired results, while simultaneously resulting in competing SOC networks also adopting new technology to maximise profits. (O)

The 'crime as a service' industry offers services in both cyber-dependent crimes – where technology is both a tool for committing crime and a target of crime – and cyber-enabled crime – where technology is a tool used to facilitate or commit another crime. The criminals who undertake 'crime as a service' offer services in areas including, but not limited to: image-based abuse; child abuse; violence; malware; ransomware; phishing; data; hacking and money laundering crimes. (U)

CASE STUDY

A decentralised online ecosystem offers 'crime as a service' across both cyber-enabled and cyber-dependent crime types. Their activities include the production and distribution of child sexual abuse material, extortion and sextortion of minors, ransomware and cryptocurrency theft. Chatgroups are used to target victims, to brag, to upskill and also to market and sell services. Members advertise capabilities for sale, offering escrow services and refunds if tasks are not completed to their customers' satisfaction. This lowers the technical barriers for offending by enabling and equipping criminal actors who lack technical capabilities. Notably, there are members based in Australia. (O)

SOC networks use technology to isolate, control and conceal their operations, creating a criminal environment that is both resilient and adaptive. These networks can recruit and task individuals – or coerce and extort them – into committing acts of physical violence or malicious damage. (O)

CASE STUDY

Three youths were arrested for the deliberate arson attack of a tobacco store in Queensland. Investigations indicate that they were opportunistically recruited by adult strangers who approached them on the street. The youths were offered a payment of $2,000 to carry out the arson, believed to be part of the escalating 'Tobacco Wars'. Communication between the parties occurred both face-to-face and via Snapchat. The adults provided all necessary tools and instructions to facilitate the attack. Despite the initial offer, the youths ultimately received only $190 for their involvement. (O)

Some SOC networks invest in and develop sophisticated online infrastructure to connect with illicit actors and coordinate activity securely and anonymously. SOC networks have adopted cryptocurrencies and virtual assets to obfuscate financial flows, automated bot accounts and accelerated the use of integrated payment platforms. One such online network – that had almost one million active users – facilitated $38.7 billion in illicit transactions for crime types including child exploitation, cybercrime, human trafficking and money laundering. (O)

CASE STUDY

The LabHost platform was a cyber-dependent example of 'crime as a service' that was marketed to criminals as a 'one stop shop' for phishing. It lowered barriers to entry for criminals to access cybercrime tools for which they lacked expertise to develop themselves. Through LabHost, criminals replicated more than 170 fraudulent websites impersonating reputable banks, government entities and other major organisations. These sites deceived more than 94,000 Australians into believing these websites were legitimate, prompting victims to disclose sensitive information – including one-time pins, usernames, passwords, security questions and passphrases – compromising their security. An international investigation identified more than 100 suspects in Australia who used LabHost to target Australian victims. (O)

The ability of intelligence and law enforcement agencies to infiltrate illicit marketplaces, intercept communications and trace illicit fund flows is impacted by the use of bespoke technologies. SOC networks target technologists for recruitment to develop bespoke encrypted communications capabilities – this includes undertaking penetration testing to challenge law enforcement and intelligence agencies' ability to identify, target and disrupt them. (O)

SOC networks involved in cyber-attacks were early adopters of services in the 'crime as a service' economy – dark web market forums, the selling of stolen data, intrusion services and criminal hosting and proxy providers – leveraging it to enable different forms of cyber-attacks. (O)

CASE STUDY

SOC networks operating as 'crime as a service' providers developed cryptocurrency-based payment systems and site-specific 'tokens' to facilitate the purchase of child abuse material (CAM). One CAM marketplace identified by the ACIC recorded a turnover exceeding US$1 million in a single year. The marketplace's transaction structure and embedded security features were deliberately designed to anonymise users and obstruct detection by intelligence and law enforcement agencies. The ACIC provided the intelligence on this 'crime as a service'-enabled CAM platform to partner law enforcement agencies for their action. (O)

The adoption of the 'crime as a service' model has also enabled foreign powers and their proxies (FPP) to leverage criminal capabilities in support of activities that foment social division and threaten Australia's national security. As the distinction between traditional nation-state operations and SOC activities becomes more blurred, FPPs may use SOC as a vector to undermine Australia's national interest, including through the use of cyber-attacks to achieve geopolitical, financial and disruptive goals. (O)

Further, the 'crime as a service' model enables sophisticated SOC entities and FPPs to distance themselves from direct involvement in crimes by employing 'cut-outs' – intermediaries who obfuscate their involvement and complicate attribution. For example, the Australian Security Intelligence Organisation recently assessed that Iran's Islamic Revolutionary Guard Corps had orchestrated attacks on Jewish interests in Australia using a complex web of proxies – including members of organised crime gangs – designed to obfuscate their direct involvement. (O)

CONCLUSION

Contracting or outsourcing criminal acts is not new. It is an entrenched practice for SOC networks that allows them to increase their reach and grow their profits across a range of illicit markets. But the use of digital technology to create online marketplaces where criminal skills can be contracted and deployed – or individuals identified, extorted or coerced into violence – is a relatively recent development. In the digital era, 'crime as a service' presents new challenges, but intelligence and law enforcement agencies are adapting and collaborating to counter the threat. (O)

Implementation of the *Independent Review of the Australian Criminal Intelligence Commission and associated Commonwealth law enforcement arrangements* will strengthen the national response to the SOC threat by ensuring the ACIC has the appropriate legislative frameworks, powers and capabilities to produce more actionable and targeted intelligence in support of partner disruption and response activities. Further, Electronic Surveillance Reform will modernise relevant legislative frameworks to accommodate technological advancements and put intelligence and law enforcement agencies on a stronger footing to combat adversaries who rapidly adopt and exploit new technologies. (O)

The ACIC will continue to work closely with partners to inform response activities and harden the environment to criminal exploitation. (O)