CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

SUBMISSION:

Inquiry into criminal activity and law enforcement during the COVID-19 pandemic

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: Inquiry into criminal activity and law enforcement during the COVID-19 pandemic

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) submission to the Parliamentary Joint Committee on Law Enforcement inquiry into criminal activity and law enforcement during the COVID-19 pandemic. We commend the Federal Government for its ongoing commitment to ensuring Australia remains a safe and secure nation and a leader in national responses to the global COVID-19 pandemic.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has two research programs: Critical Infrastructure Security and Cyber Security as a Service.

The CSCRC is a public company limited by guarantee and will invest $AU50 million of Australian Commonwealth Government funding and additional Participant funding over seven years to 2025 in research outcomes related to our key impact areas. The CSCRC has 24 Participants including seven Research Providers, seven State and Federal Government Agencies/Departments and 10 Industry/SMEs.

We look forward to answering any queries about this submission and welcome the opportunity to participate in future discussions regarding this very important topic.

Yours Sincerely,

Rachael Falk
CEO, Cyber Security Cooperative Research Centre
ceo@cybersecuritycrc.org.au

Executive Summary

The Cyber Security Cooperative Research Centre (CSCRC) welcomes the opportunity to provide this submission to the Parliamentary Joint Committee on Law Enforcement inquiry into criminal activity and law enforcement during the COVID-19 pandemic. Such an inquiry is timely and pertinent given the widespread impact that the global pandemic is having on our digital world, both offline and online.

COVID-19 has highlighted the interconnectedness of the world we live in and the vital importance of our law enforcement agencies during times of great upheaval. COVID-19 has also demonstrated the central role that the digital world plays in our lives, reaching into every aspect of society. As workers around the world have rapidly moved to less cyber secure, remote working conditions, there has been a simultaneous rise in online criminal activity and brazen acts of cyber exploitation. As a liberal democracy, Australia has a proud tradition of charting an effective course between maintaining the rule of law and adhering to democratic checks and balances, and the CSCRC has every confidence that our nation will continue to do so. Therefore, it is essential that during this period of uncertainty, amid growing online threat vectors and a proliferation of cyber threat actors, our law enforcement agencies are equipped with the appropriate measures to adequately respond to the rapidly changing world of online criminal activity.

There is a clear opportunity for Australia to ensure domestic laws – laws with real-world consequences – are aligned with cyber and digitally-perpetrated developments. This will enhance Australia's reputation as a world leader in cyber security and as a nation at the forefront of efforts to tackle cyber security threats.

The CSCRC submits:

- there should be no difference between the online or offline environment when it comes to rule of law and the recognition of criminal activity
- that the Australian Government continue to take a vocal stance on cyber deterrence policies and mechanisms to disincentive cyber threat actors in the immediate future
- that the Australian Government and the responsible law enforcement agencies continue to reinforce alignment with our Five Eyes allies in 'calling out' illegal cyber behaviours
- that domestic law enforcement agencies be equipped with the appropriate powers necessary to operate in a challenging threat environment in a proportionate and timely manner to prevent and prosecute cybercrimes.

Our submission responds to the following:

The nature and operations of transnational, serious and organised crime, including the impact of border controls and other policy responses to the pandemic that have impacted supply chains and the movement of goods and people, and tactics adopted by criminal organisations to adjust to or exploit changes in their operating environment during the pandemic.

The COVID-19 lockdown period has witnessed an exponential rise in cyber activity by malicious cyber actors.[1] These actors are conducting nefarious activity against organisations, governments and the Australian public. The increase in activity is reflective of the less cyber secure working conditions that predominate for workers globally, now largely working from home. The surge in reliance on home networks and systems has made it increasingly difficult for organisations to mitigate cyber risk. To this end, the CSCRC contends that there should be no difference between the online or offline environment when it comes to rule of law and recognition of criminal activity. Abiding by this principle will serve to enhance trust in Australia's cyber systems both internationally and domestically.

COVID-19 is unfolding against the backdrop of rising geopolitical tensions and increased global protectionism, as cyber criminals seek to exploit new vulnerabilities and wreak havoc across existing supply chains. Australia has not been spared. In May 2020, the Australian steel maker, BlueScope Steel, suffered a crippling ransomware attack that severely impacted the company's global operations. The attack, which occurred in the company's US systems, had global impacts, even affecting BlueScope operations at the Port Kembla plant in NSW.[2]

2020 has brought a series of high-profile cyber attacks on Australian businesses. Logistics company Toll endured two malware attacks in early 2020. Lion Dairy and Drinks, Australia's largest brewing and dairy manufacturer, was forced to halt production after a June 2020 cyber attack disrupted its entire supply chain and threatened to impact newly reopened Australian pubs.

[1] https://www.cyber.gov.au/acsc/view-all-content/media-releases/unacceptable-malicious-cyber-activity
[2] https://www.abc.net.au/news/2020-05-15/bluescope-steel-cyber-attack-shut-down-kembla-ransomware/12251316

The CSCRC commends the concerted effort by governments, Australia included, to move away from the primacy of existing overseas supply chains to secure sovereign products and services and to decouple, technologically, from nations that may pose a threat to our sovereignty. The CSCRC notes that these actions will help to ensure the future security of Australia's critical infrastructure and national security and notes that it offers Australia the opportunity to position itself as a global leader in procuring sovereign technology solutions.

How the pandemic has affected the prevalence of certain types of crime, particularly crime types associated with transnational, serious and organised crime
&
Trends and changes in relation to other crime types of specific interest to Commonwealth law enforcement agencies, including but not limited to fraud and cyber-crime.

Considering these two issues together, the CSCRC contends that COVID-19 and the subsequent global lockdown period has resulted in a sharp surge of malicious cyber activity and cyber crime, on several fronts.

First, COVID-19 has underscored the interconnected nature of our digital world and the challenge of securing citizen data and our digital economy. Under COVID-19, large, transnational companies with operations in Australia are finding it more challenging to secure networks and prevent cyber threats with the vast majority of staff now working from home under less secure, remote working conditions. Furthermore, many workers are now relying on their personal networks to conduct business with far-flung colleagues, entailing frequent network interactions with overseas jurisdictions that are subject to differing sets of governing laws and regulations. Cyber criminals, bound by no territorial, sovereign jurisdiction, are acutely aware of this and are seeking to exploit these newfound threat vectors. The Australian Cyber Security Centre (ACSC) has published a series of COVID-19 cyber advisories to the public during this period, outlining the increase in pandemic-related phishing email scams and online fraud attempts. The CSCRC commends Commonwealth law enforcement agencies, together with the ACSC, for their vigilance during this period. The Australian Government has demonstrated world-leading responsiveness to these cyber threats, underscoring to the Australian public the tangible ways that malicious cyber activity may impact their personal well-being and how citizens can mitigate cyber risk.

Furthermore, as noted in the recently released Industry Advisory Panel Report into the 2020 Cyber Security Strategy, transnational cybercrime syndicates and their affiliates, who develop, share, sell and

use increasingly sophisticated tools and techniques, are of growing concern.[3] Such groups operate at scale, targeting individuals and organisations by exploiting vulnerabilities. The report highlights an expected surge in business email compromises, cryptocurrency mining, credential harvesting and ransomware, noting "ransomware is a particularly grave threat because it disrupts the operations of businesses and governments by encrypting files and demanding a ransom for their return. Recovering from such incidents is almost impossible without comprehensive backups".

Second, COVID-19 has highlighted the nebulousness of geopolitical boundaries induced by a borderless, transnational cyberspace, which largely exempts malicious cyber activity from local laws and regulations and continues to allow nefarious cyber actors to navigate cyberspace with impunity. Concurrent to the global pandemic, there has been a rise in hostile cyber activity conducted by a variety of cyber threat actors (state-based actors, cyber criminals, terrorists) with novel types of targets. For example, in the global race to secure a COVID-19 vaccine, covert cyber espionage is being undertaken by rogue nation states who are exploiting the pandemic environment to obtain COVID-19 vaccine data from overseas researchers.[4] To this end, the CSCRC recommends that the Australian Government continue to take a vocal stance on cyber deterrence policies and mechanisms to disincentive cyber threat actors in the immediate future.

The CSCRC also recommends that Australia continues to align with our Five Eyes allies in calling out harmful cyber behaviours. Australia is fortunate to have strong international strategic and trade ties. The longstanding Five Eyes alliance between Australia, Canada, New Zealand, the United Kingdom and the United States has historically formed the backbone of Australia's national and economic security and COVID-19 has sharpened its focus on cyber security. In June 2020, the countries signalled their commitment to a unified response concerning pandemic-related malicious cyber activity and online disinformation campaigns.[5] Australia's relationship with other strategic allies, based on collaboration, participation and openness, will play a vital role into the future.

The nature and effectiveness of responses by law enforcement to trends and changes in criminal activity related to the pandemic, including any changes in the practices, methods and procedures of law enforcement.

[3] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf, page 17
[4] https://www.homeaffairs.gov.au/news-media/archive/article?itemId=428
[5] https://tech.newstatesman.com/security/five-eyes-alliance-covid-19-cyber-attacks

Changes that might be desirable, in light of any current and possibly longer-lasting trends and changes in criminal activity related to the pandemic, and in view of the preparedness of Commonwealth law enforcement in undertaking its work during the pandemic, to the functions, structure, powers and procedures of the Australian Federal Police and the Australian Criminal Intelligence Commission.

Concerning the rise in cyber threats since the beginning of COVID-19, the CSCRC contends that although there are international norms, conventions and treaties that govern global cyberspace and state behaviour, the transnational nature of cyberspace remains an impediment to law enforcement agencies, still bound by Westphalian conceptions of sovereignty and the state. Malicious cyber activity is frequently inflicted from beyond sovereign borders and domestically bound laws and regulations, allowing many cyber actors to elude due process and prosecution for their crimes. Furthermore, such activity is not always conducted at the behest of the state and, as previously noted, actors may be taking directives from underground crime syndicates and terrorist organisations. This continues to be a hindrance to law enforcement agencies.

The CSCRC commends the Australian Government for recent public denouncements of bad cyber behaviour(s) in cyberspace and for its demonstrated commitment to continue to draw attention to this type of activity. The June 2020 announcement by the Morrison Government highlighting a 'sophisticated, state-based actor' targeting Australian organisations,[6] and the July 2020 Australian Government agencies' joint statement in support of the recent UK-US-Canada Joint Cyber Security Advisory, condemning recent Russian cyber espionage pertaining to the COVID-19 vaccine, are case in point.[7]

Despite these actions, legislation still lags behind technological developments. The CSCRC contends that Australian law enforcement agencies should be equipped with the appropriate powers necessary to operate in a challenging threat environment in a proportionate and timely manner to prevent and prosecute cyber crimes. This includes consideration of legislative changes that allow Australian law enforcement agencies lawful access to data and devices where appropriate. Cyber criminals and their illegal activities cannot be allowed to flourish because of a perceived principle that privacy of communications is paramount.

[6] https://www.lowyinstitute.org/the-interpreter/morrison-s-messages-sophisticated-state-based-cyber-actor
[7] https://www.homeaffairs.gov.au/news-media/archive/article?itemId=428

The extent to which trends and changes in criminal activity during the pandemic, and related changes to law enforcement methods, practices and procedures, might endure beyond the pandemic.

The heightened awareness and spotlight shone on malicious cyber activity and the impact of cyber crime on the lives of Australian residents, businesses and government entities during COVID-19 has had an unexpected silver lining. Cyber crime and harmful cyber behaviours are no longer ephemeral, as they largely were pre-pandemic. They are now real and tangible issues that bear on the wider Australian populace.

The Australian Government has been a world leader in national responses to the more pronounced cyber threat environment that has proliferated under COVID-19, offering measured and proactive responses to bolster our nation's cyber security resiliency. In the international sphere, the CSCRC urges the Federal Government and responsible law enforcement agencies to continue demonstrating leadership in this capacity and has every confidence that Australia will remain committed to the development of and adherence to international cyber norms and values, many of which are premised on the same democratic ideals this nation was founded upon. The CSCRC believes this adaptive public response to ever-evolving changes in cyber threats has cast a much-needed and effective spotlight on the tangible impact of cyber security across the minutiae of our lives.

The Federal Government has demonstrated the pandemic will have an enduring impact on Australia's cyber security posture, with the implementation of a number of key measures that will shape our nation's future cyber security resiliency. In June 2020 the Morrison Government announced a decade-long $1.35B investment in cyber security capability – the Cyber Enhance Situational Awareness and Response (CESAR) package.[8] This expenditure will provide a critical boost to the nation's cyber capabilities and aid efforts to thwart rising cyber security threats. The investment also takes aim at the human capital front, seeking to expand Australia's cyber security workforce which suffers from a critical shortage of talent. Furthermore, the forthcoming Australian Cyber Security Strategy has been revised, allowing relevant government departments to incorporate key learnings from the COVID-19 pandemic and altered environment for cyber security threats.

There is an opportunity for Australia to be a global leader in cyber security law and policy. It is vital the Federal Government continues to pursue its stated aims regarding legal principles which are applicable

[8] https://www.pm.gov.au/media/nations-largest-ever-investment-cyber-security

for both the online and offline world.[9] Australia has led the way globally with legislation such as the *Telecommunications and Other Legislative Amendments ('Assistance and Access') Act 2018* and the *Criminal Code Amendment (Sharing of Abhorrent Violent Material*) *Act 2019*, which are appropriate responses to an environment where organised crime, terrorism, and fraud are frequently amplified, inspired and facilitated online.

[9] https://www.theaustralian.com.au/commentary/encrypted-messages-favour-the-worst-of-the-worst/news-story/3fc80e3c44341f0a11f85824df0f7bcc