Northern Territory Police Force

OFFICE OF THE COMMISSIONER

Committee Secretary
Parliamentary Joint Committee on Law Enforcement
Via Email: le.committee@aph.gov.au

Dear Committee Secretary

INQUIRY INTO THE CAPABILITY OF LAW ENFORCEMENT TO RESPOND TO CYBERCRIME

Thank you for your correspondence dated 24 October 2023, regarding this Inquiry and the opportunity to make a submission on behalf of the Northern Territory Police Force (NTPF). Please find attached the NTPF submission.

I welcome the considerations of the committee regarding both the legislative opportunities required, and the capacity for law enforcement and industry to respond to community needs to facilitate greater protection against cybercrime.

Should you have any further queries, please contact Detective Acting Superintendent via email

Commissioner of Police

2 January 2024

Northern Territory Police Force

Inquiry Submission

INQUIRY INTO THE CAPABILITY OF LAW ENFORCEMENT TO RESPOND TO CYBERCRIME.

In relation to correspondence received on 24 October 2023 regarding the Inquiry into the capability of law enforcement to respond to cybercrime, please see the Northern Territory (NT) Police Forces' written submission below:

a. Existing law enforcement capabilities in the detection, investigation and prosecution of cybercrime, including both cyber-dependent crimes and cyber-enabled crimes;

The NT Police Force maintains a Cybercrime Unit staffed by one Sergeant and one Constable. This provides a limited capability for NT Police to detect, investigate and prosecute cybercrime, including both cyber-dependent and cyber-enabled crimes. The Cybercrime Unit monitors and receives reports from the ReportCyber portal, through which the NT Police Force receives the vast majority of reports of cybercrime. The Cybercrime Unit triages these reports, conducts investigations and provides victim support. Where the offender is NT based, the Cybercrime Unit undertakes prosecutions through the criminal courts.

The Cybercrime Unit relies heavily on the Joint Policing Cybercrime Coordination Centre (JPC3) and interstate police assistance to investigate more complex cybercrime matters and where the offender/s are not NT based.

Acknowledging the resource constraints that this genre of offending poses, the need for staff with specialised skillsets and training opportunities for law enforcement officers is critical, as the demand for this skillset is not yet met by available resources.

b. International, federal and jurisdictional coordination law enforcement mechanisms to investigate cybercrimes and share information related to emerging threats;

International, federal and jurisdictional coordination of law enforcement mechanisms to investigate cybercrimes and share information related to emerging threats is coordinated by the Australian Federal Police (AFP) via the JPC3 located in Sydney, and the Operation Helios Joint Management Group, which meets quarterly and is a forum to share information and investigative techniques.

Obtaining data from overseas must currently be done via the Mutual Legal Assistance Treaty process. The AFP coordinate this process via Interpol, and the local law enforcement agency then serve warrants on behalf of the requesting agency. This process can be very slow (18 – 24 months for turnaround). However, the introduction of the US *Clarifying Lawful Overseas Use of Data Act*, or "CLOUD Act", and the signing of the *Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* (commonly referred to as the Australia-US CLOUD Act Agreement), will ultimately change this to an International Production Order (IPO) process. NT Police are currently undergoing the process to become an "Accredited Agency" to enable use of this Agreement.

IDCare is an organisation contracted to provide an identity and cyber incident community support service. IDCare also provides regular intelligence alerts on criminal operators and groups and their methodology as part of their ongoing monitoring of security interests.

Work is currently underway regarding how information from Scamwatch (National Anti-Scam Centre) may interact with and be included into the ReportCyber portal. Opportunities present to ensure that the National Anti-Scam Centre and Scamwatch information enhances rather than duplicates the information and efforts of ReportCyber and the JPC3.

NT POLICE SUBMISSION - INQUIRY INTO THE CAPABILITY OF LAW ENFORCEMENT TO RESPOND TO CYBERCRIME

c. Coordination efforts across law enforcement, non-government and private sector organisations to respond to the conduct of cybercrimes and risks of cybercrime;

As above, the AFP undertakes the vast majority of this coordination through the auspices of the JPC3 and Operation Helios. For example, the JPC3 has taken the lead in coordinating a response to cyber security incidents of national significance, such as the Optus data breach.

d. Emerging cybercrime threats and challenges affecting Australian entities and individuals, including the scale and scope of cybercrimes conducted in Australia or against Australians;

The threat of cybercrime to Australian interests has escalated in profile and impact year on year, and poses an evolving and increasingly sophisticated challenge to Australian Federal, State and Territory governments, as well as Australian businesses and individuals.

In the NT, businesses have been regularly targeted through Business Email Compromise (BEC). BECs have caused losses to businesses and individuals in the NT ranging from tens to hundreds of thousands of dollars. Some NT based businesses have also suffered from ransomware attacks. Phishing, spear-phishing and social engineering are used by cyber-criminals to target businesses and exploit vulnerabilities.

The largest financial harm to individuals in the NT is currently being caused by cryptocurrency investment scams. A number of individuals have suffered significant losses. These range from several hundred thousand dollars each, to one notable NT victim losing $4.98 million in 2022 to this type of scam. It is important to note that whilst for many victims who lose less than one hundred thousand dollars, the impact of such a loss is still very significant to the individual and their family. It is extremely difficult for police to recover funds once they have been transferred to these fake investment companies. The level of personal harm through anguish and embarrassment leads to distinct under reporting of these events.

Many individuals in the NT have become victims of intimate image sextortion. Young males aged from mid-teens to late twenties are most often the victims of this sort of extortion. In some extreme cases interstate, this has led to the victim suiciding.

Romance scams also have a significant impact on individuals in the NT. This can lead to financial loss when the victim sends money to the scammer, but can also lead to the victim becoming a “money mule” for money laundering purposes when the scammer asks the victim to receive and then transfer money through their own bank account. Individuals living in remote NT communities appear to be particularly vulnerable to being recruited as money mules.

There is a dire need for improved awareness and understanding by businesses and the general public in how to protect against and inform on cyber security and cybercrime elements. The under-reporting of such crime through fear of reputational damage, professional or personal embarrassment, shame or misunderstanding of the nature of the offending is capitalised on by criminal entities to progress their offending and actions.

e. The opportunities and challenges of the existing legislative framework in supporting law enforcement to investigate and act upon instances of cybercrime;

Current NT legislation is not fit for purpose in the digital age, particularly in the areas of searching and seizing digital devices, digital evidence and cryptocurrency. This has resulted in, wherever possible, NT Police partnering with the AFP to allow the use of Commonwealth digital search powers as a work-around of the archaic NT legislation. There is currently no policy, procedure or requisite legislation for the seizure of cryptocurrency in the NT.

NT POLICE SUBMISSION - INQUIRY INTO THE CAPABILITY OF LAW ENFORCEMENT TO RESPOND TO CYBERCRIME

Law enforcement can be further impeded by the accessibility of lawful access to encrypted communications and devices. It would be welcomed if further consideration be given to ensuring law enforcement can meet community expectations in managing offending that is empowered through the use of such communication platforms and devices.

The prosecutorial environment is incredibly complex due to the variation in state and federal legislation, and the borderless, often trans-national aspect of the types of offending.

An opportunity exists for legislative review at both the NT and Federal level. Ideally, a Legislative and Policy Review Committee would examine policy, procedure and legislation of all Australian jurisdictions and internationally, with the goal of creating draft national uniform legislation and best practice policy and procedure that can be adopted by all jurisdictions. National uniform legislation would strengthen interoperability and partnerships between jurisdictions, nations, and industry. A very high level of agility, interoperability and jurisdictional cooperation, nationally and internationally, is of critical importance in identifying the rapid changes in technology, offence patterns and cyber threats to Australian governments, businesses and individuals, and in preventing and combating these threats.

..End..