PARLIAMENTARY JOINT COMMITTEE ON LAW ENFORCEMENT

INQUIRY INTO THE CAPABILITY OF LAW ENFORCEMENT TO RESPOND TO CYBERCRIME

Australian Federal Police

Written questions on notice

Senator Polley asked the following questions on Tuesday 4 June 2024:

1. The committee understands that the Joint Policing Cybercrime Coordination Centre (JPC3) focuses on high harm, high volume cybercrime. Can you please elaborate on this? How does the JPC3 identify and select the cases it will dedicate most resources towards?
2. The committee heard that the Australian Federal Police (AFP) may not have the mandate to investigate scams *(Committee Hansard [Proof]*, 23 May 2024, pp. 23, 26). Could you please clarify whether, and how, the AFP investigates online scams?
3. The committee heard there may be benefits in notifying cyber security companies about cybercriminal activity, to allow them to update their firewalls and protect users from the vulnerability *(Committee Hansard [Proof]*, 23 May 2024, pp. 32–33). Can you please advise what level of threat information the AFP or JPC3 shares with industry?

The response to the senator's question is as follows:

1. Legislation and national law enforcement arrangements determine the triaging process and ultimately which Australian law enforcement agency will have responsibility for investigating the offence. This is also applied to cyber-enabled scams reported to law enforcement via ReportCyber. Under these national processes, the AFP:
    a. investigates cybercrime against the Australian Government, critical infrastructure, systems of national significance or those that impact the whole of the Australian economy.
    b. provides support and advice both internally and to law enforcement more broadly, to deal with the intersection of crime and technology.
    c. coordinates with domestic and international law enforcement on prevention and awareness raising campaigns and the promotion of available government resources designed to protect individuals and mitigate potential cybercrime threats.

   The response to "high harm, high volume" cybercrime includes a combination of cybercrime investigations and target development, disruption, and prevention activities into a range of cyber-dependent and cyber-enabled crimes which include, but are not limited to, the following;

    - business email compromise;

- phishing/smishing;
- unauthorised access/modification/impairment of data;
- attacks against critical infrastructure;
- cyber enabled investment fraud/scams;
- remote access fraud/scams;
- bank impersonation fraud/scams;
- money muling, identity theft and misuse of personal identifiable information;
- sextortion;
- malware; and
- distributed denial of service.

Given the public/private model, the AFP-led JPC3 implements to combat cybercrime through collaboration, the prioritisation of these matters can be influenced by a range of factors including harm to the Australian community, ReportCyber arrangements and global trends and/or joint investigations with foreign law enforcement partners, state and territory police partners, private sector partner referrals, or target development. It is the national coordination of this effort and Australian policing response that is key to JPC3 role and success.

Noting the above and given the broad and pervasive nature of cybercrime, the JPC3 determines the resourcing for each case based on several dynamic factors, including community harm and the impact law enforcement can have to combat cybercrime at scale. Once the AFP receives a report of crime, it is internally assessed against a consequence scale to determine the impacts of cybercrime ranging from insignificant, minor, moderate, major to severe.

2. The term 'scam' is generally quite broad and can intersect with numerous crime types, at both the Commonwealth and state/territory level.

   The ACCC's National Anti-Scam Centre (NASC) coordinates the national response to scams, working with industry, regulators, law enforcement agencies, and community organisations to make it more difficult to scam Australians.

   The AFP is engaging with the NASC in a number of areas including through a NASC secondee at the AFP-led JPC3, membership of the NASC Advisory Board and membership of a number of NASC working groups and fusion cells. The AFP is committed to protecting Australians from scams as part of this response.

   The AFP works collaboratively with government and industry partners as part of the coordinated response to scams and will investigate and respond where it falls within the agency's remit to do so.

This can include targeting cybercriminals and money laundering syndicates that enable organised crime groups, including those carrying out systematic scams. Often, there is a strong cybercrime nexus in the methodology of scams.

The JPC3 capitalises on the policing powers, experience and investigation and intelligence capabilities of all Australian policing jurisdictions and partner agencies to inflict maximum impact on high harm, high volume cybercrime affecting the Australian community, which can include high volume scams.

Recent examples of this include:

a. JPC3 leading Operation Dolos which is an ongoing multiagency taskforce targeting business email compromise (BEC) scams – Operation Dolos has prevented over $66 million in losses since it was established in 2020.

b. A recent high-profile sextortion scam case reported in the media leveraged the JPC3's technical capabilities and partnerships with the FBI and AFP's South African Post to identify the offenders, who have been arrested and charged locally in South Africa.

3. The AFP works closely with our partners including the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) and the Department of Home Affairs to raise awareness about cyber security vulnerabilities and enable information to be shared with industry through the publication of alerts, advisories or notifications.

   While other Commonwealth agencies lead on the notification of cyber security vulnerabilities to industry, the AFP engages in proactive prevention initiatives and public awareness campaigns to inform and educate the Australian community about cybercrime threats and how to protect themselves online. For example, AFP Cyber Command has issued media releases on topics such as ransomware, COVID-19 related scams, romance scams, remote access trojans, sextortion, and online child exploitation, providing advice and tips on how to avoid becoming a victim of these crimes.

   The AFP also participates in national and international events, such as Safer Internet Day and Fraud Week, to raise awareness and promote best practices for cyber security and resilience. The AFP believes that prevention is important, and that a collaborative approach with industry, government, and the public is essential to combat cybercrime effectively and efficiently.