AFP
AUSTRALIAN FEDERAL POLICE

Parliamentary Joint Committee on Intelligence and Security

Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

April 2021

Supplementary submission by the Australian Federal Police

Introduction

1. The Australian Federal Police (AFP) welcomes this opportunity to make a supplementary submission to the Committee's review of the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (SLAID Bill).

2. This supplementary submission provides additional operational context to highlight the importance of certain aspects of the Bill as drafted, which is suitable for a public submission (noting the Committee has received a detailed, classified briefing from the AFP). The submission also responds to Questions on Notice taken by the AFP during the public hearing on 10 March 2021.

The threat environment

3. The increase in criminality and harm occurring online continues to be of significant concern to law enforcement agencies, particularly because the rapid evolutions in digital technology has left the current legislative framework out of step with the criminal environment.

4. The SLAID Bill will provide the AFP and the Australian Criminal Intelligence Commission (ACIC) with additional powers to tackle the increasing use of anonymising technology by serious criminals, including highly-sophisticated organised criminal syndicates.

5. To bring any investigation to prosecution, police need to know the fundamentals: who and where the offenders are, and what they are planning. Our ability to gain this vital information is increasingly challenged, and no single legislative amendment can wholly address this. Only by ensuring law enforcement agencies have a wide variety of powers that can be deployed in concert can this be addressed.

Anonymising technology – continuing challenges and limitations

6. Anonymising technology prevents communications being attributed to specific individuals by concealing locations and other identifying information. This provides an additional layer of privacy to that afforded by obscuring communications with encryption. These technologies are most commonly associated with dark web services, dedicated encrypted communications platforms, virtual private networks (VPNs) and some 'Over-the-Top' application providers (e.g. Telegram or other encrypted messaging applications).

7. Anonymising technologies generally employ forms of encryption to assist in concealing where a user or service is hosted, but not all encryption provides anonymity. This is why powers designed to address the issue of encryption may not always help law enforcement overcome an offender's use of anonymising technologies.

The evolution of the internet and anonymising services and its impact on law enforcement

8. Originally, traditional interception under a warrant would reveal all the information required to identify an individual, their location and any criminal content (such as message content, sender and recipient details, and accurate IP addresses and locations).

9. Now, the combination of encryption and anonymising technology has drastically shifted the technological environment in which law enforcement operates. Encryption renders the content of many communications unintelligible while in transit over the telecommunications network, while readily-available anonymising technology, such as VPNs, means accurate details about the sender and recipient's identities and locations may not be ascertainable.

10. Law enforcement efforts to identify individuals committing offences, their location, and the type of criminality occurring online, become extremely difficult, with very limited information available through lawful interception methods.

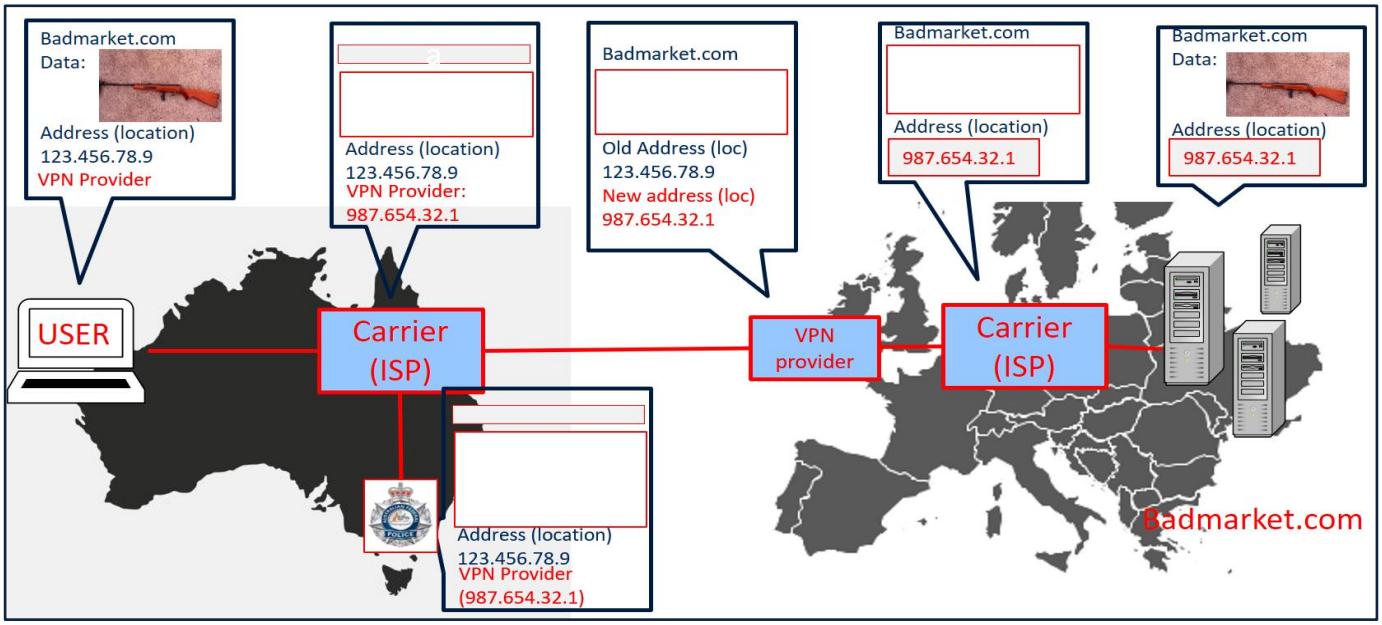

***Figure 1**: Reading from right-to-left, the available information originating from the user is rapidly obscured as the message transmits from the sender to the recipient. The carrier (who executes the interception warrant for the AFP) can only see the VPN provider IP address and the recipient's IP address. Only the seller and purchaser can see the full content of the message – details of firearms being illegally trafficked into Australia.*

Dedicated encrypted communications platforms

11. The intersection of encryption and anonymising technology is most evident in the various Dedicated Encrypted Communications Platforms (DECPs) designed for, and marketed to, organised criminals as tools to avoid law enforcement detection.

12. Organised criminal networks increasingly use DECPs to facilitate a wide variety of serious offending. This is not just limited to large-scale drug production, importation and distribution, but also includes money laundering, stolen and fraudulent identities, crypto-currency exchanges and instructions on how to establish accounts and businesses, and avoid border and customs detection.

13. DECPs are typically modified handsets that have ordinary functions removed (including standard SMS, calls and internet browsing). Instead, bespoke applications for encrypted messaging, calls and notes are pre-installed to ensure communications between handset owners can occur securely and anonymously.

14. Law enforcement agencies, through using the industry assistance framework introduced by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA), are generally able to identify how many of these devices are being used throughout Australia. However, due to sophisticated security mechanisms, we are unable to identify who is using these devices, or where they are being used. When lawful interception is attempted, very little useable data is able to be received by law enforcement.

15. This is a problem because we know DECPs are being widely used. Overseas takedowns of platforms, such as PhantomSecure and Encrochat, has identified criminals openly discussing and organising their criminal operations on DECPs, because they believe this information cannot be monitored or attributed to them. This is not limited to chat conversations, but also other information valuable to law enforcement, such as images to confirm deliveries and locations of the illicit goods and services in which they deal, as well as banking information and stolen or fraudulent identity information.

16. Providers of DECPs are often active in providing support to their users as to how to avoid further detection in the wake of law enforcement takedowns. For example, in June 2020, when Encrochat realised their servers had been compromised, the company released messaging to its users, advising them their activities may have been compromised and steps they should take to avoid law enforcement detection.

Figure 2: *Images openly shared by offenders in Europe discussing their criminal behaviour across the Encrochat platform, including drugs, money and a shipping container equipped as a torture chamber. Encrochat also advised platform users that their system had been compromised and how to avoid detection.*[1]

[1] Sources: *Liverpool Echo (https://www.liverpoolecho.co.uk/news/liverpool-news/drug-dealer-traded-cocaine-heroin-19770318), BBC News (https://www.bbc.com/news/uk-england-merseyside-55916153), Bloomberg (https://www.bloomberg.com/news/articles/2020-07-16/european-police-hacked-secret-phone-network-used-ai-for-major-bust) and Europol (https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe)*

Additional AFP case studies

17. The SLAID Bill will enable the AFP to more effectively address the technical challenges facing our priority crime types, including child protection, cybercrime and terrorism. The below case studies provide further detail about how the SLAID Bill will benefit these investigations.

Child Protection investigations – use of account takeover warrants (ATW) and data disruption warrants (DDW)

18. The AFP, including through the AFP-led Australian Centre to Counter Child Exploitation, has witnessed a **significant increase** in online child abuse offending over the last 12 months, particularly due to the impact of COVID-19 restrictions and increased time spent online.

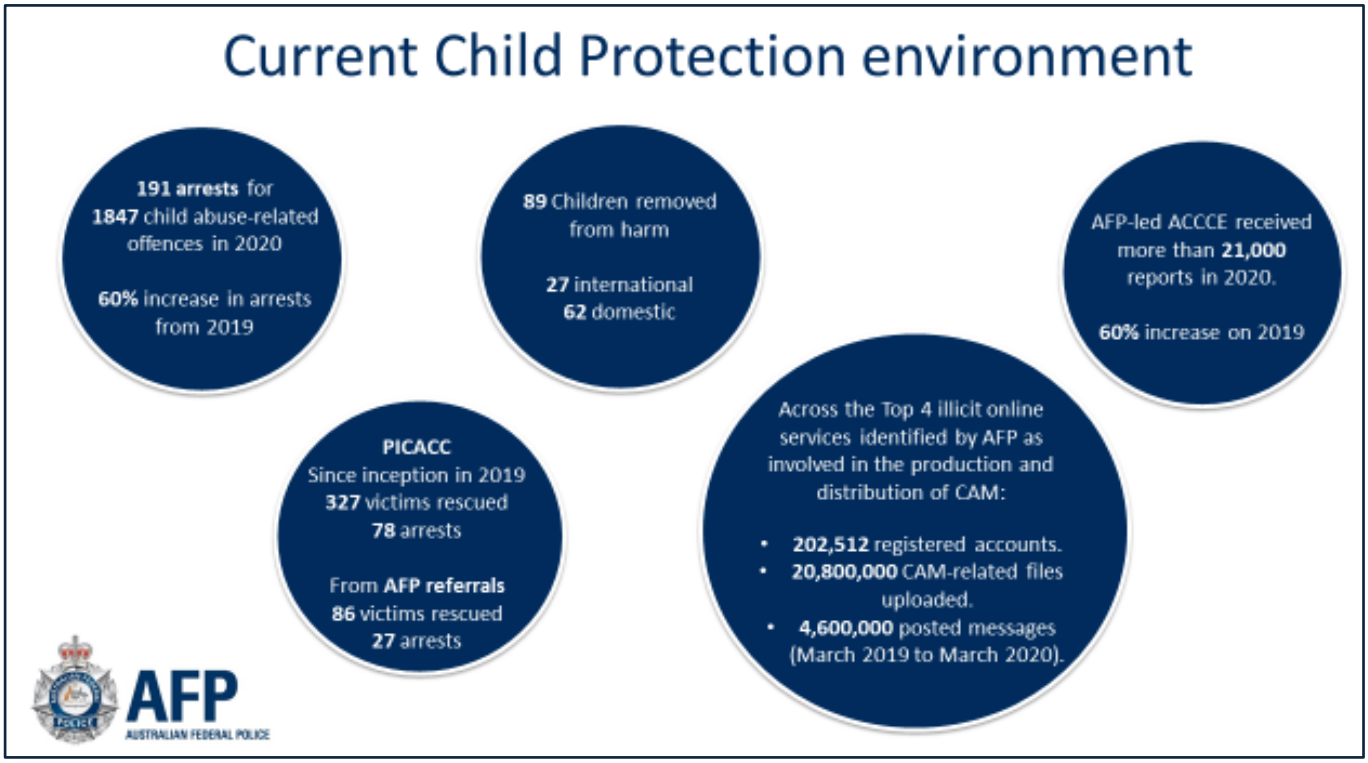

Figure 3: *The extent of the problem faced by the AFP and one of our international partners, the Philippine Internet Crimes Against Children Centre (PICACC) during 2020.*

Account takeover warrants

19. Currently, it is critical that investigators move promptly to secure online accounts during a search warrant, to prevent content being deleted by an offender, or prevent other perpetrators in the network being alerted to police interest (either by the offender or through media coverage). The absence of a clear authority for law enforcement to involuntarily take over an offender's accounts presents several other significant challenges.

Figure 4: *Use of online accounts and encrypted communications by child abuse offenders presents significant challenges for the AFP in securing vital evidence or identifying additional offenders.*

20. When used in child protection investigations, account take overs will help address some of these challenges, primarily by lessening the risk offenders will:

    - Not provide their consent to a takeover, or will retract their consent at inopportune moments, potentially halting valuable avenues of investigation and evidence collection (as can currently occur when an offender risks facing a harsher sentence); and

    - Delete key evidence or notify criminal associates in the early moments of a search warrant resolution (if demonstrated to the issuing officer that the ATW is necessary to enable evidence to be obtained regarding commission of the serious offences). This could be where a covert account takeover will prove useful, where the takeover is to be performed prior to resolution of a search warrant.

21. By enabling the AFP to take control of an offender's account, an ATW will also provide alternative avenues to remove child abuse material from an offender's online, cloud-based accounts, or prevent others accessing that material, where the AFP has another warrant or other power authorising this action (for example, a DDW).

Case example

22. Account takeovers, when used in conjunction with controlled operations, will provide the AFP with additional opportunities to infiltrate networks of child abuse offenders in order to identify other offenders – a significant boost to the AFP's covert engagement work.

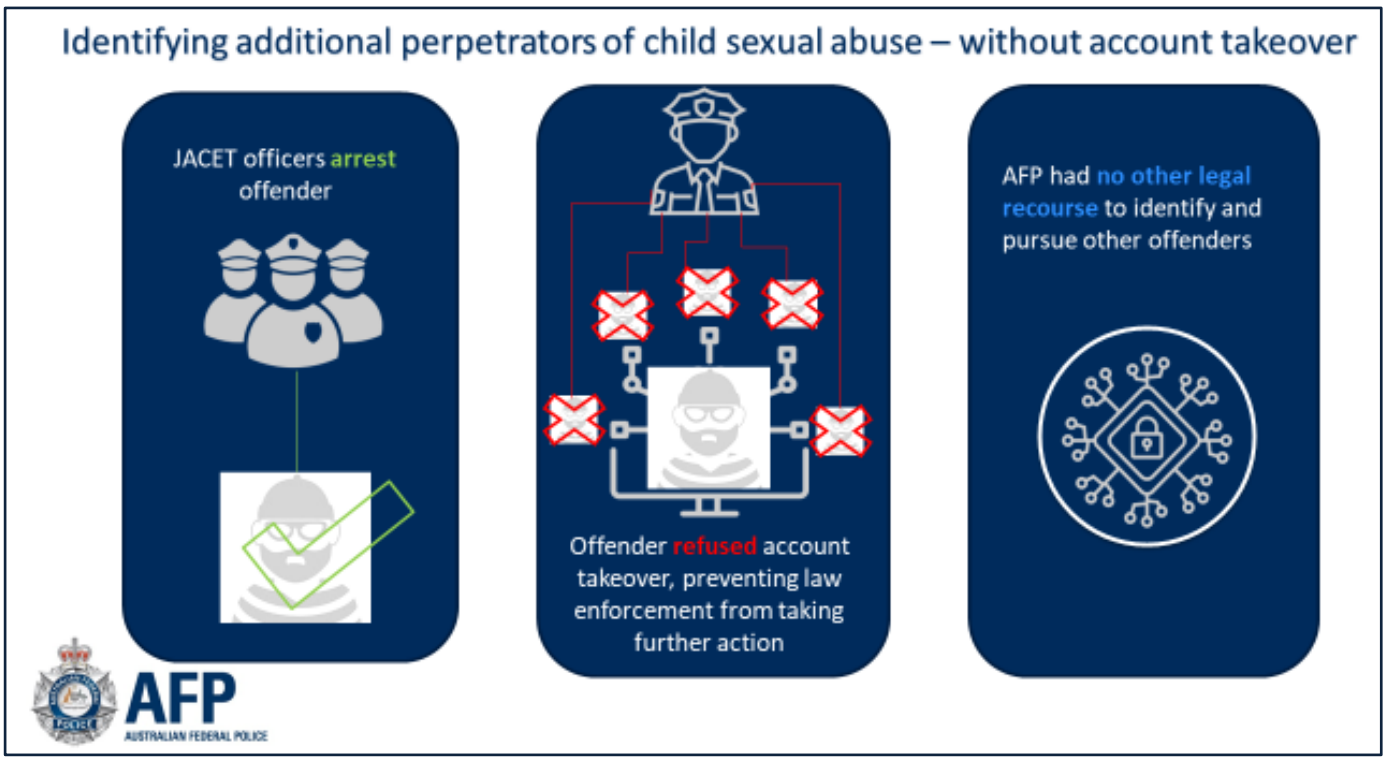

Figure 5: *If an offender does not consent to an account takeover the AFP loses valuable opportunities to gain access to the criminal network and identify other offenders and victims.*

For example, in 2020 a Joint Anti-Child Exploitation Team, comprising members from the AFP and state police, arrested an Australian man for allegedly sexually abusing a number of children, and distributing videos recording this abuse on an instant-messaging and social networking app. We allege the scale of abuse was extensive, with more than 100 charges laid, including 'producing child abuse material for use through a carriage service' (under section 474.23(1)(a)(ii) of the Criminal Code) and other serious Commonwealth offences.

Analysis of the individual's instant-messaging app identified communications between the alleged offender and other users, during which they received and transmitted child abuse material, including through live-streaming. However, the encrypted 'over-the-top' instant messaging app used by the accused allowed the use of pseudonyms to obscure users' true identities. When combined with use of a VPN, account holders could operate with almost complete anonymity.

The AFP sought the alleged offender's consent to take over his account for the purpose of identifying others engaged in procuring and sharing child abuse material. The man refused, and now other perpetrators who shared child abuse material from the alleged offender, or requested it from him, cannot be readily identified.

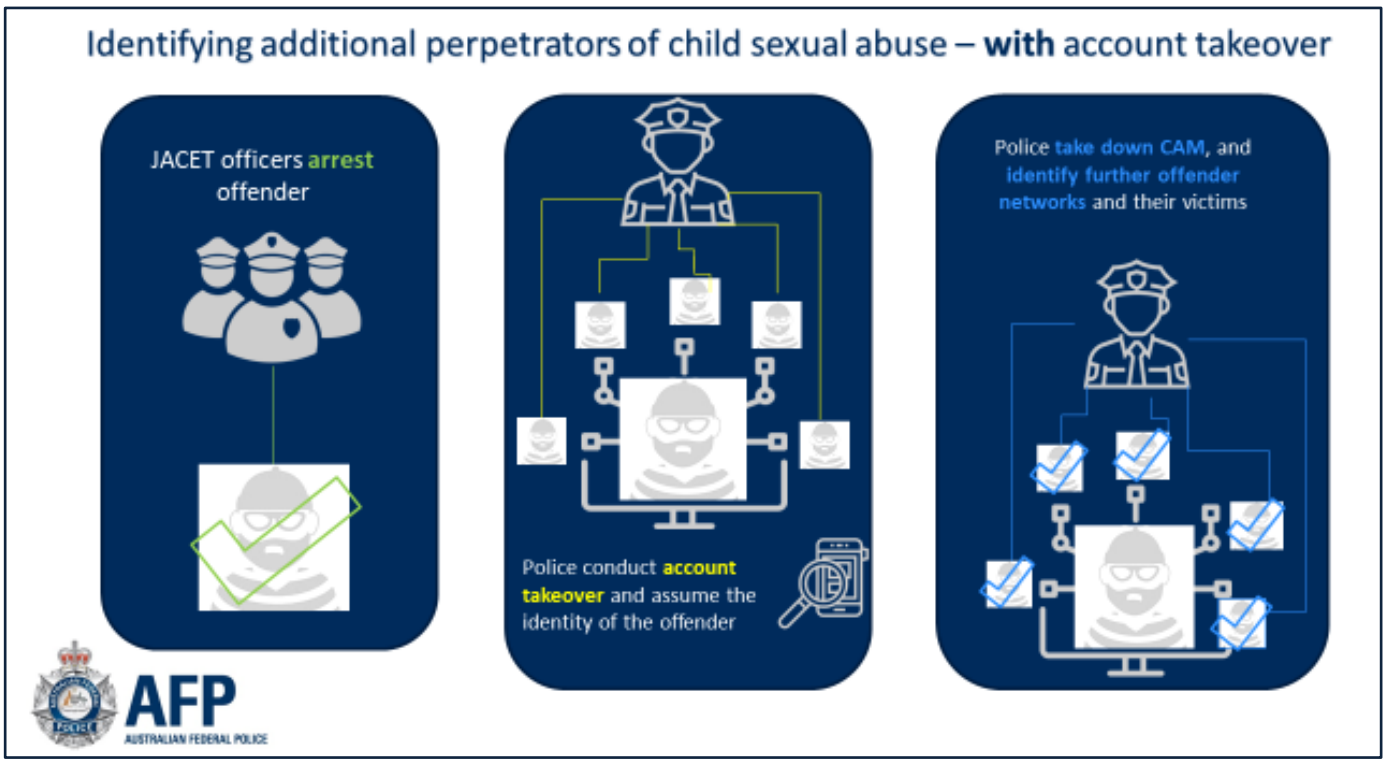

Figure 6: *In this case, an account takeover warrant would have provided AFP with greater scope to identify other users who were involved in the production and distribution of child abuse material, and take down or close accounts used to distribute this abhorrent material. This would have occurred in conjunction with a controlled operation, to authorise assuming the offender's identity and necessary covert engagement.*

Data disruption warrants

23. The ability to frustrate offending by disrupting or modifying data held in computers will present new opportunities for the AFP to target services distributing child abuse material. The below diagrams outline a current AFP investigation where abuse material is being shared on a large-scale, amongst a vast number of unidentified users.

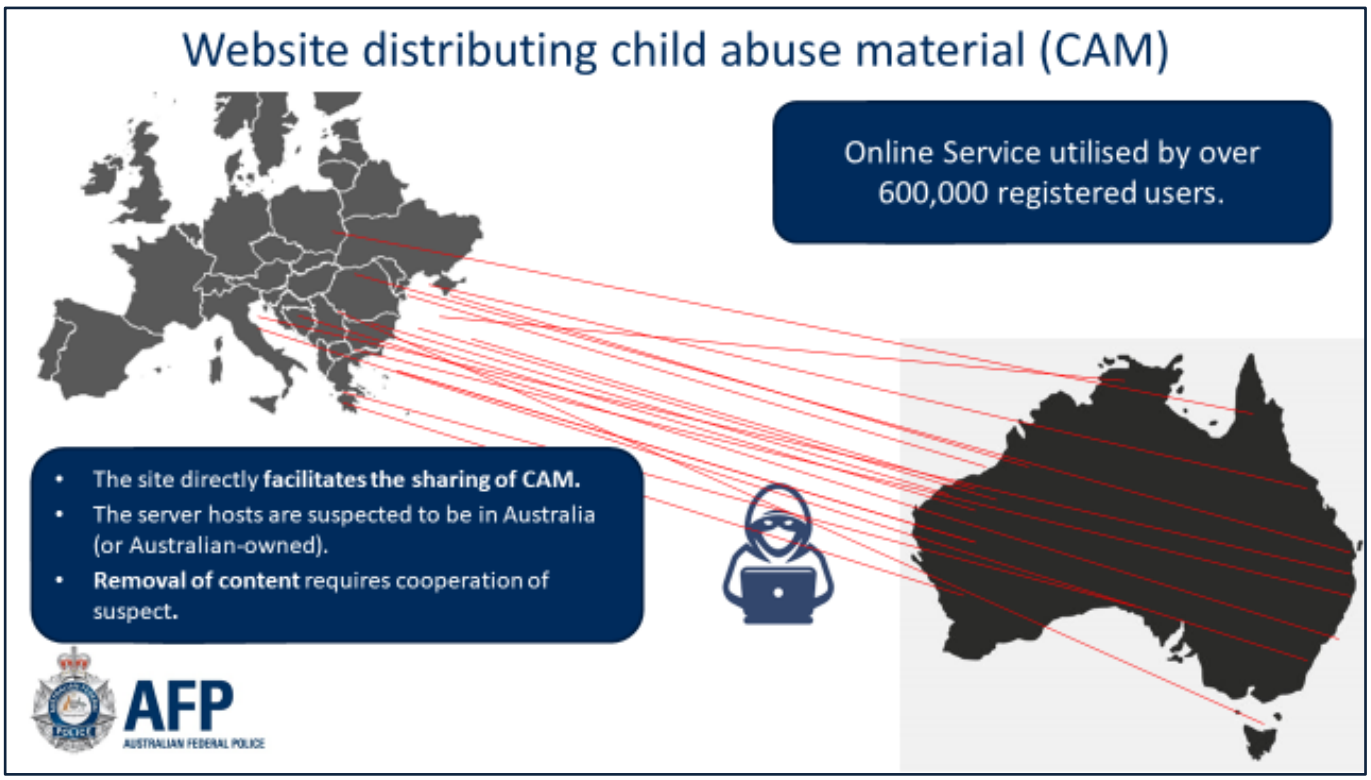

Figure 7: *At present, the AFP have no options to remove the child abuse material (CAM) hosted on this service, as users are currently unidentified.*

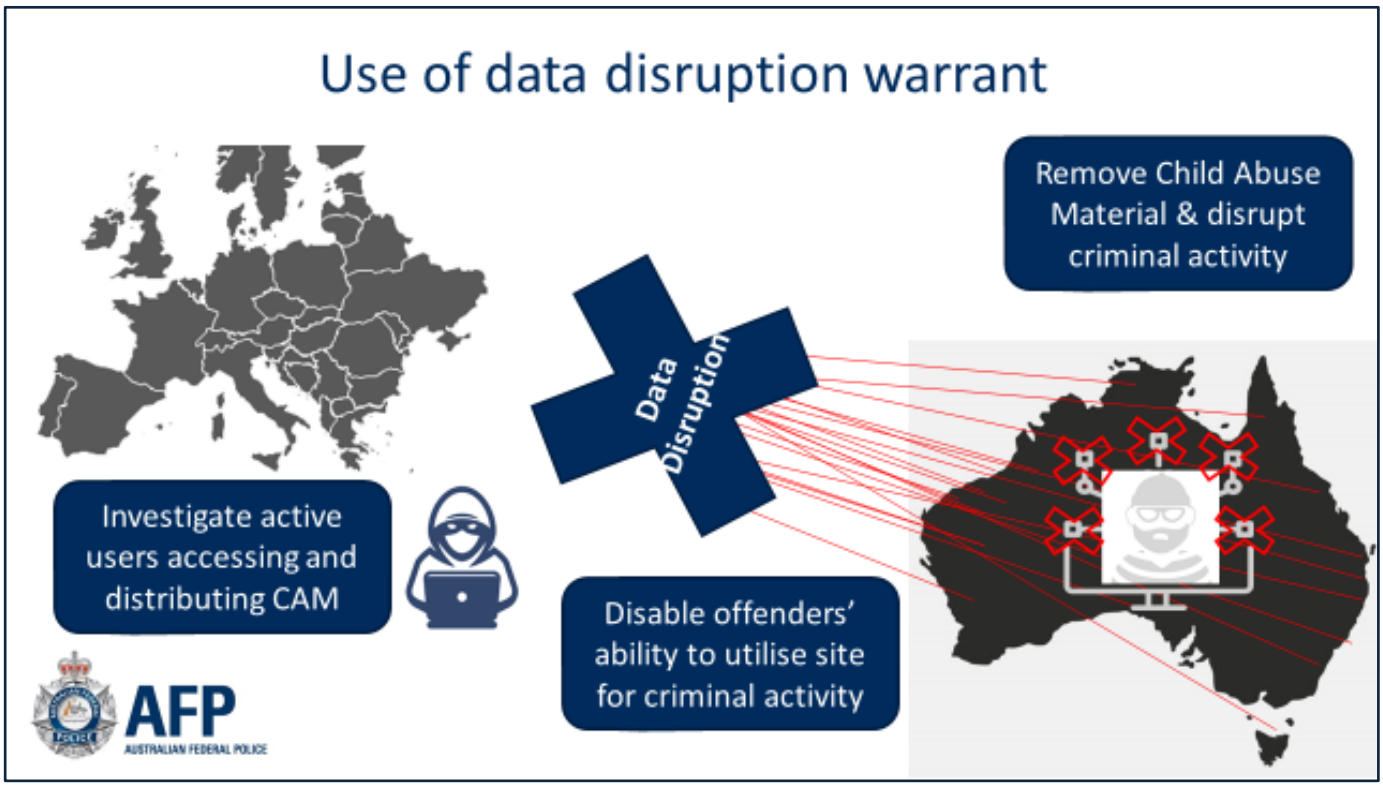

Figure 8: *The AFP could apply for a* ***data disruption warrant****, enabling the AFP to remove CAM from clear or dark web services and disrupt users' continued access and distribution of the material. This would not prevent the AFP continuing to investigate the registered and active users, but the CAM would be taken down and removed from the server, preventing further victimisation of children*

Cybercrime investigations – use of data disruption warrants (DDW)

24. Malicious cyber activity is increasing and poses a direct threat to Australia's national interests, economic prosperity, and the financial and physical security of everyday Australians. Australia is an attractive and profitable target due to our relative wealth, concentrated banking sector, high levels of online connectivity and increasing delivery of services through online channels. For example:

- In 2018, the estimated direct economic loss from cyber security incidents for Australian businesses was **$AUD 29 billion** per year (Microsoft and Frost & Sullivan estimate);
- In 2019, Australians lost more than **$634 million** to scams, according to the Australian Competition and Consumer Commission; and
- There were around 5,600 cybercrime reports to the government's 'ReportCyber' website per month in the 2019-20 financial year, which is only one reporting source, and likely underrepresents the total number of cyber and cyber-enabled crimes across Australia.

25. The type and volume of online frauds and other cyber-enabled crimes which have arisen following recent crises, such as the 2019-20 bushfires and the COVID-19 pandemic, highlights the adaptability of increasingly tech-savvy criminals.

Case example – Remote Access Trojans (RATs) and AFP Operation Cepheus

26. Operation Cepheus was an AFP investigation into the distribution and use of the 'Imminent Monitor Remote Access Trojan' (IM-RAT). While this investigation was a success for the AFP, the proposed data disruption warrants would have provided a greater ability to protect the Australian community from the harmful effects of this malware.

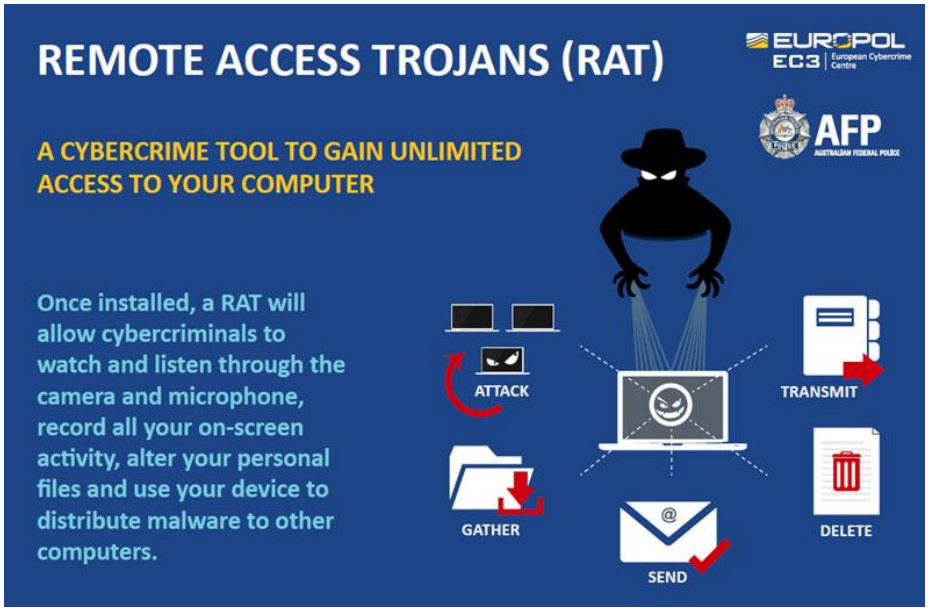

Figure 9: *RATs allow criminals to stalk victims, steal personal information (ID fraud), steal credentials (enabling theft) and intellectual property, and exploit children and vulnerable persons. Many RATs can be purchased relatively cheaply, and do not require much technical knowledge to use. RATs can also be custom-made for 'clients' – cybercrime as a service.*

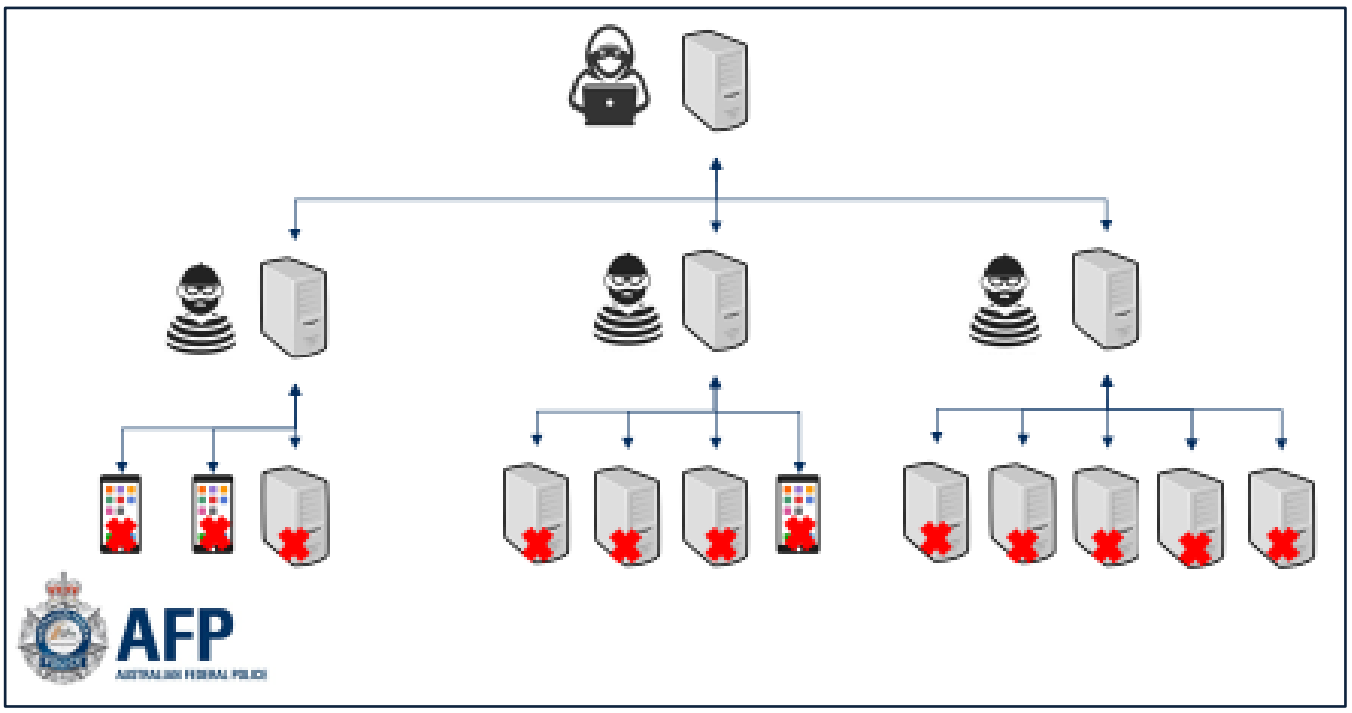

Figure 10*: *Distribution and use of the 'Imminent Monitor Remote Access Trojan'.

The offender (top of diagram) develops the malware and then sells an IM-RAT licence to other criminals, providing 'controller software' to the purchaser. IM-RAT licences were sold on forums dedicated to hacking and criminal use of malware, for as little as $US25.

The controller software allows the criminal's device to act as a Command and Control server; the criminal then infects innocent victims' computers and other devices with the RAT, using methods including phishing. The criminal using the controller software then has remote access to the victims' device and can control it as desired.

The AFP's investigation uncovered a network supporting the distribution and use of IM-RAT across 124 countries, with sales records showing there may be more than 14,500 purchasers. While the true number of victims is unknown, it could be in the tens of thousands (globally).

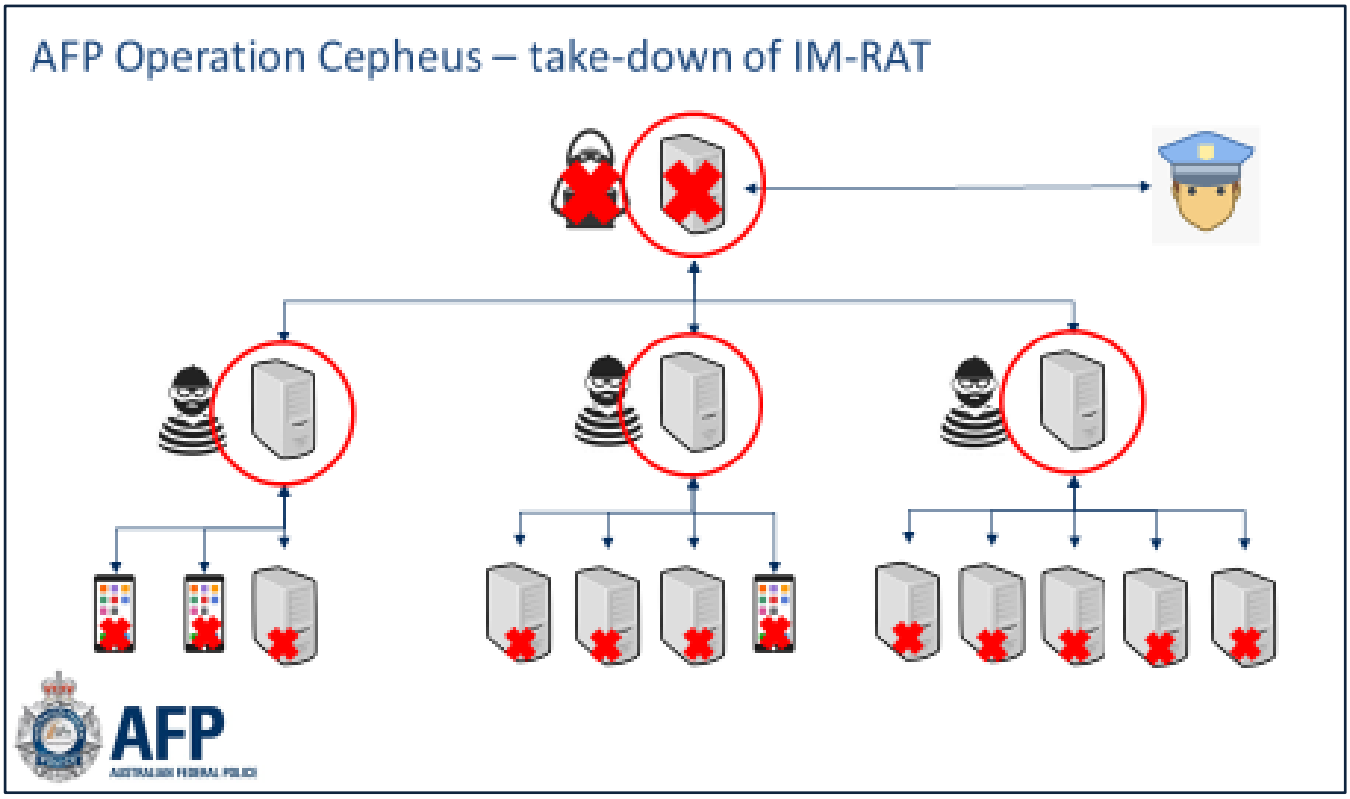

Figure 11: *Following a lengthy investigation, the AFP identified the servers used by criminals to distribute and use the IM-RAT. The AFP was ultimately able to take down the RAT, making it more difficult for criminals to use the malware. The AFP also shut down the website selling the IM-RAT licences, preventing further purchases of the tool and potential misuse, preventing new crimes and victims.*

However, the AFP's current warrant powers only permit evidence collection, and nothing could be done alter the IM-RAT to frustrate the commission of further offences and remove it from victim devices.

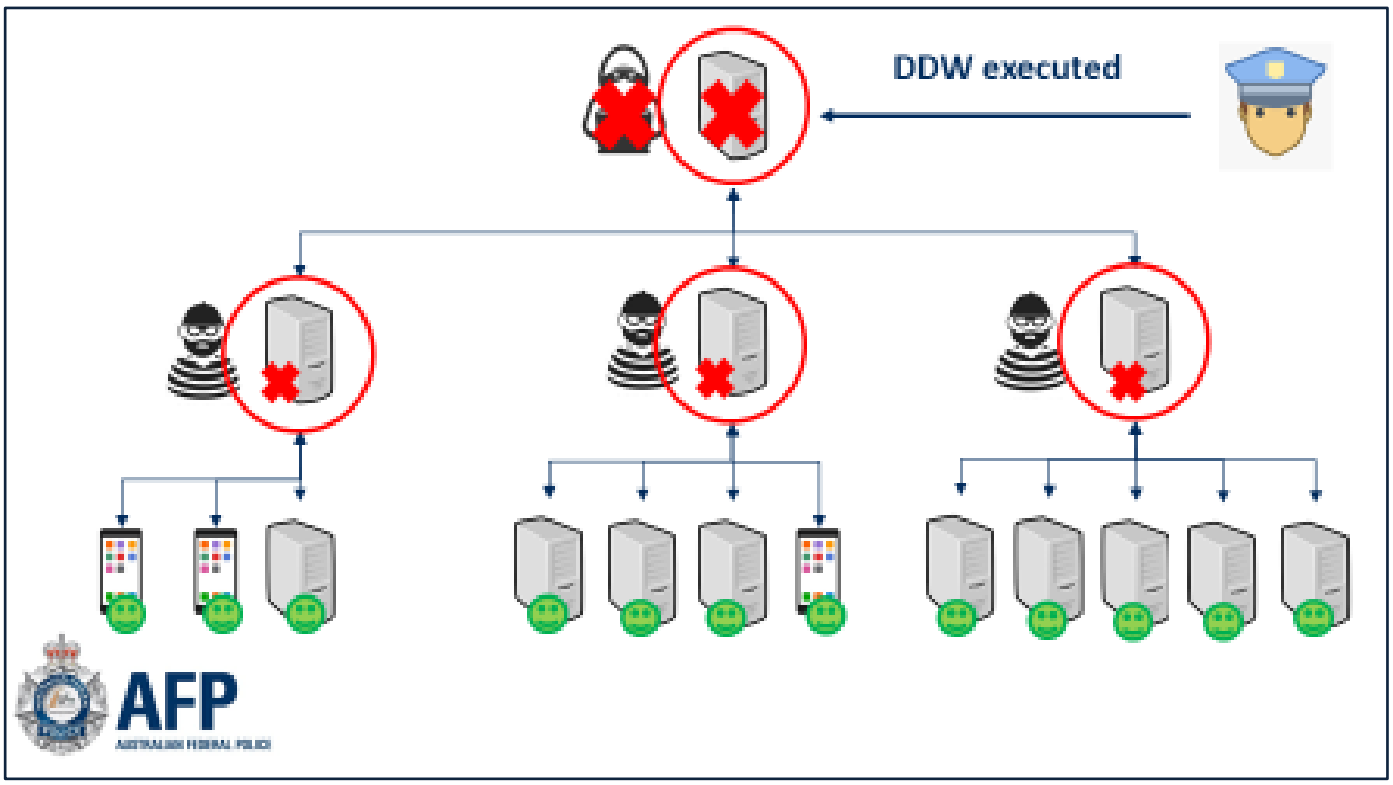

***Figure* 12:** *By using a data disruption warrant, the AFP would be able to gain access to the servers used by the criminals using the malware. Then, using the ability to modify data in a computer the AFP could make changes to the RAT software on those servers, in a manner which would cause the removal of the RAT from the victims' computers. This would enable the AFP to better protect the Australian community from the wide variety of offending facilitated by use of RATs.*

Counter-terrorism investigation – Use of network activity warrants (NAW)

27. The rapid development of anonymising and encrypted technology is also changing the counter-terrorism environment, and presents new challenges for the AFP in addressing this threat. For example, increased online connectivity allows for the globalisation of extremist views and groups, and the proliferation of online content inciting and threatening violent action.

28. The vast range of encrypted messaging platforms now available also provides many options for anonymity and typically persons of counter-terrorism interest often use multiple platforms and communications options to avoid law enforcement detection. There is also a level of fluidity in these groups, as membership on these online platforms fluctuates. The combined impact of these factors is that it becomes incredibly challenging for law enforcement to positively identify persons of interest, understand the scope and scale of their global links, and efficiently gather sufficient information to meet the threshold to use existing warrants.

29. Network activity warrants, along with other powers in the SLAID Bill, will provide additional opportunities to reduce the threat to public safety and work against the radicalisation of individuals by enabling earlier intelligence collection and investigation into unknown individuals and their connections. This will allow the AFP to take early disruptive action, enhance our ability to collect admissible evidence, and help identify links to other crime types (for example, any nexus between individuals with extremist views and organised crime).

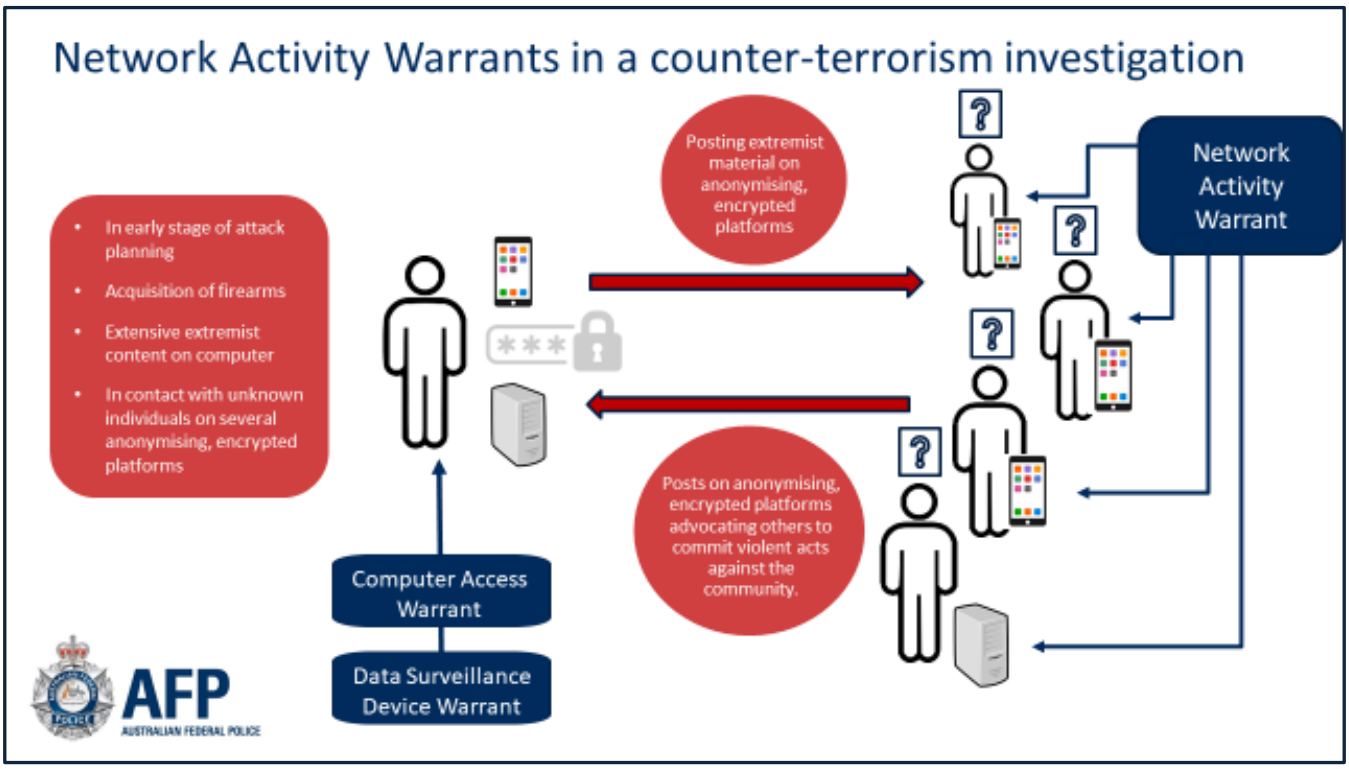

***Figure 13**: **Potential use of Network Activity Warrants**. In this case, the AFP is aware of an individual who is in the early stages of attack planning and is in communication with a number of unknown individuals using various encrypted messaging platforms.*

While the AFP could use a Computer Access Warrant to access data on the main suspect's devices, a Network Activity Warrant will allow the AFP to gather intelligence about the broader network of individuals who are using the encrypted platform to advocate violent extremism. This will enable the AFP to access devices used by the unknown individuals over the life of the warrant, even if they move between different encrypted platforms. Intelligence gathered could include the identities of these individuals, the scope of their network, and any further criminal planning.

AFP use of the Assistance and Access Act 2018 (TOLA)

30. The powers in the SLAID Bill will **enhance the options** available to the AFP and the ACIC to **target, uncover and combat** serious offenders who disguise their criminal activities through technology and harm the Australian community.

31. However, our existing powers and frameworks remain useful, and the AFP anticipates the SLAID Bill powers will be complementary. We expect to use these new warrants alongside existing powers, assistance frameworks, technical capabilities and our longstanding relationships with partner agencies.

32. In particular, the assistance and access framework established by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA) will remain an important mechanism and will continue to complement the new powers.

AFP interaction with industry through the assistance and access framework

33. The AFP has issued nine (9) Technical Assistance Requests (TARs) since the industry assistance and access framework commenced in December 2018. These requests were issued to assist the AFP's investigations into cybercrime, organised crime, drug trafficking and importation, as well as telecommunications offences.

34. Further, the AFP does not believe the proposed assistance orders in the Bill (proposed section 64B of the SD Act for DDWs, and section 3ZZUV of the Crimes Act for ATWs) either replicate the TOLA industry assistance framework, or allow the AFP the circumvent the legal protections and certainties provided by TOLA.

35. The new assistance provisions for DDWs and ATWs must be issued by an external issuing officer, not the AFP, unlike the TOLA industry assistance framework. These new provisions will be to compel identified named individuals (not industry) who have knowledge of specific target computer systems or online accounts, to provide reasonable assistance necessary to disrupt or access data, or access an online account.

36. For example, the AFP could seek assistance orders from a computer owner, account holder or a system administrator, including, but not limited to, suspected offenders.

37. The AFP would not use these provisions to target individual employees of a particular provider. In circumstances where those employees would fall within the category of persons who could assist, the AFP would use TOLA to seek the assistance on the designated communications provider, not individual employees. The AFP will continue to use TOLA where available, if we require further technical assistance from industry in order to execute or give effect to a warrant (like we currently do with CAWs, as appropriate).

AFP internal processes for warrant applications

38. Some public submissions have raised concerns that any AFP member can apply for a data disruption or account takeover warrant (in contrast with the 'chief officer' applicant required for network activity warrants).

39. The AFP rejects suggestions this would lead to a 'junior' or inexperienced officer applying for, and executing, a DDW or ATW without appropriate oversight or training.

40. In practice, in the AFP's warrant applications do not occur without oversight from more senior ranked or commissioned AFP officers. Depending on the type of warrant, AFP internal governance requires warrants to be reviewed by a more senior member and potentially accompanied by a capability or execution plan, which require advice from multiple AFP areas.

41. For example, an internal 'Special Projects Committee' will examine and approve all proposed AFP warrant applications under the SD Act (such as surveillance devices and computer access warrants) and the *Telecommunications (Interception and Access) Act 1979* (TIA Act) before the application is made. Special Projects Committees generally involve two Superintendents (EL officers) vetting the application, and are a critical internal mechanism to ensure all warrants (and any supporting affidavits or other documents) are given due consideration.

42. These oversight procedures are necessary because warrant applications are only one part of an investigation, alongside numerous other internal considerations, such as the broader investigative strategies, agency operational priorities and resourcing. The AFP takes a coordinated approach to allocating staff, technical and specialist capabilities, as these must be considered before a warrant application can be made. These processes require extensive planning, and cannot be initiated by any given officer acting alone.

43. Similar strict internal governance will be developed for DDWs and ATWs, particularly given the cost and sensitive capabilities which will likely be required to execute the warrants

(particularly DDWs) and the intended use of ATWs alongside controlled operations (which are internally authorised by AFP SES members).

AFP applicants for DDWs and ATWs

44. From an operational perspective, it is preferable that warrant applicants for DDWs and ATWs are not restricted to only 'senior' or commissioned AFP officers.

45. As with most existing warrants available to the AFP, the warrant applicant should be the officer who is primarily responsible for the investigation, as they will be most familiar with details of the investigation and will be in charge of compiling the information and intelligence required to obtain the relevant warrant. They will be required to satisfy the issuing officer that the warrant threshold requirements are met, and will be in the best position to answer any questions from the issuing officer.

46. DDWs and ATWs will also be used in conjunction with other powers, and mandating a more senior applicant will create significant complexity, delay and administrative burdens to the process if multiple different applicants are required. For example, an ATW is likely to be sought at the same time as a section 3E search warrant, where the applicant can be at the constable level. It could create logistical delays for an investigation if the warrant applications require both a constable and superintendent (EL2 level) to be present.

47. As the AFP stated at the public hearing, an AFP member's rank within the organisation is not necessarily reflective of their operational and investigative experience. There are many members within the AFP with an apparently 'junior' rank who hold many years of significant policing experience.

AFP internal training for warrant applicants and authorising officers

48. The AFP has a number of internal training and governance procedures to ensure all members who are eligible to apply for warrants, or authorise the use of powers, are familiar with their legislative obligations. This includes ensuring members understand the powers available under legislation, their statutory obligations and threshold requirements, any reporting obligations and oversight (for example, by the Commonwealth Ombudsman), the importance of legislative compliance (and adverse consequences for non-compliance) and how to find assistance and resources to meet obligations.

49. This training must be completed before members can apply for certain warrants or authorise the use of certain powers (including all powers under the TIA Act and SD Act). The AFP will create similar compulsory training for DDWs, ATWs and NAWs.

50. Within the AFP, the Covert Analysis and Assurance (CAA) section also supports AFP investigations by ensuring compliance with relevant legislation governing telecommunications interception, data authorisations, surveillance device warrants, computer access warrants, controlled operations and delayed notification search warrants.

51. CAA is also responsible for record-keeping, reporting services, and facilitating the Commonwealth Ombudsman's oversight of the various legislative regimes. In the AFP's experience, the Commonwealth Ombudsman is very particular in requiring agencies to demonstrate they have processes and training in place to ensure that any member exercising powers overseen by the Ombudsman (which include powers under the SD Act, TIA Act and Crimes Act 1914) have a strong understanding of the legislative requirements and relevant considerations for use of intrusive warrant powers.