AFP
AUSTRALIAN FEDERAL POLICE

Parliamentary Joint Committee on Intelligence and Security

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

February 2021

Submission by the Australian Federal Police

Introduction

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

2. The AFP strongly supports the SLAID Bill and was extensively consulted during its development. The SLAID Bill empowers the AFP to more effectively fulfil our mission to protect the Australian community and cause maximum damage to the criminal environment, by introducing three new warrants designed to identify and frustrate offenders who are committing serious, cyber-enabled crimes.

3. The AFP has already commented extensively to this Committee, and the broader community, our significant concerns regarding criminal use of encryption, anonymising technology and the dark web. We can see the impacts of crime in our community, but are increasingly challenged in identifying who the criminals are, where they are, and the *exact* nature of their criminal activity. This lack of visibility results in serious cyber-enabled crimes occurring with impunity, and with global reach.

4. In his 2020 report on the *Telecommunications Legislation Amendment (Assistance and Access) Act 2018* (TOLA), the former Independent National Security Legislation Monitor, Dr James Renwick commented:

> '*just as we do not accept lawlessness in the physical world, we should not accept lawlessness in the virtual world. Therefore, in principle, the surveillance powers that apply in the physical world should also apply to the virtual world unless there are good reasons that they should not*.'

5. The AFP agrees serious crimes should not be immune from prosecution merely because Australia's laws have not kept pace with technology to apply equally to the physical and virtual or digital world, allowing criminals to exploit technology and operate outside our reach.

6. Exploitation of technology by criminals also challenges our ability to achieve another vital aspect of our work – disruption. The AFP has long considered disruption in law enforcement as the *delaying, diverting or otherwise complicating* the commission of crimes or the operations of a criminal entity. Many different operational tactics and strategies can be used to effect a disruption, and it may be the most appropriate response, either when securing a successful prosecution in Australia is not feasible, or when disruption interrupts harm and prevents it from continuing—for example, in human trafficking, counter-terrorism, drug imports and instances of anonymous but trackable offending. To date, the AFP has extensively disrupted criminal enterprises through traditional policing activity, such as arresting offenders to disrupt plots and dismantle syndicates, intercepting illicit goods trafficked across our borders, working with international partners to rescue victims of child abuse, and damaging the business model of serious crime (including by seizing the instruments and proceeds of crime). However, as crime increasingly transfers to the digital world, so too must our powers evolve to ensure we can continue to disrupt criminal threats, wherever they emerge.

7. We acknowledge encryption and anonymising technology are important tools for protecting the privacy and data of Australians. However, these tools are also used on a daily basis to enable and hide serious criminal activity, including child abuse, terrorism

and violent extremism, trafficking of illicit substances and firearms, and the sale of malware and stolen personal identification.

8. As technology continues to advance at an incredible rate, the harm posed to the Australian community will only grow. For example, the AFP-led Australian Centre to Counter Child Exploitation (ACCCE) identified, between April and June 2020, a **163 per cent increase** in child abuse material downloaded on the dark web, compared to the same period in 2019. Each image shared by these anonymous users represents a child subjected to abhorrent and reprehensible abuse.

9. The new powers in the SLAID Bill will significantly enhance the options available to the AFP and the ACIC to overcome technological obstacles and take appropriate action against those who harm the Australian community. Combined with existing AFP and ACIC technical capabilities and other legislative powers, the SLAID Bill will allow us to more effectively **target, uncover and combat** criminals who use the dark web and anonymising technology to facilitate and disguise their criminal activities.

10. However, no legislation is a 'silver bullet', and challenges will remain in this environment. We welcome consideration of all and any measures that strengthen the law enforcement response to cyber-enabled crime, safeguarded by appropriate thresholds and oversight mechanisms. There is even more that can be done, particularly to modernise Australia's telecommunication interception framework to support intelligence-gathering activities. We will continue to work with our partners to advocate for powers which appropriately remove obstacles to investigations and allow us to cause maximise damage to the criminal environment.

11. The AFP is not alone in seeking to address the threat posed by the dark web and anonymising technologies. Collaborative, international efforts are essential to combating this threat. For example, German law enforcement's recent takedown of Dark Market, suspected to be one of the largest dark web illegal marketplaces to-date, demonstrates how global, coordinated law enforcement efforts can have great success in identifying and targeting dark net marketplace hierarchies. The AFP supported this global effort and investigations are ongoing.

12. The AFP is working closer than ever with domestic and international partners to enhance Australia's cyber capabilities and create a high-risk, hostile environment for cyber criminals, both onshore and offshore. The powers introduced by the SLAID Bill will help the AFP build on our strong, long-term international relationships, and enhance our ability to contribute to the global fight against transnational serious and organised crime threats, which is essential to keeping Australians safe online.

13. Finally, the AFP acknowledges industry and the Australian public may want to better understand the scope of these powers, and the actions they permit the AFP and ACIC to undertake. We are conscious of the responsibility and trust the Australian public places in the AFP as Australia's Commonwealth policing agency. The powers proposed in the SLAID Bill, while new in the context of the online environment, have an equivalent effect to existing law enforcement responses, and are appropriate when considering the complexity and increasingly global scale of cyber-enabled crime. There are also extensive oversight provisions, ensuring our use of these powers is transparent and held to a high standard.

14. The AFP recommends this submission be read alongside the Home Affairs Portfolio submission to this inquiry. The Portfolio submission provides policy rationale and context

for the SLAID Bill, while this submission focuses on the operational context, including real case studies to demonstrate the challenges faced by law enforcement with respect to the dark web and anonymising technologies, the types of criminal activity facilitated, and how these powers will assist AFP investigations. The AFP was extensively consulted on the Portfolio submission.

15. The AFP thanks the Committee for the opportunity to provide this submission and would be happy to appear before the Committee to discuss this submission or the SLAID Bill further.

The threat environment

16. Increasing criminal use of the dark web and anonymising technology facilitates a wide array of serious, cyber-enabled crime, while creating significant challenges for law enforcement in identifying and locating offenders, and gathering admissible evidence.

17. Firstly, the terms 'dark web' and 'anonymising technology' are not synonymous. 'Anonymising technology' refers to those technologies which can disguise a person's activities, location and true identity, while the 'dark web' refers to areas of the internet which cannot be accessed without specialised browsers or other software. These concepts are often linked, because anonymising technology is required to access the dark web.

18. From the AFP perspective, both issues present significant challenges for law enforcement, as they both facilitate a wide variety of criminal activity, while providing offenders with the cloak of anonymity. The intersection of these issues is particularly concerning when investigating offences involving child abuse material.

Anonymising and encrypted technologies

19. Rapid advances in technology over the last decade, and its increasing ease of use and affordability (in many cases, at no cost), have provided a myriad of ways for criminals to hide their identity and avoid traditional law enforcement identification techniques.

20. For example, if a person is using a Virtual Private Network (VPN), their online location (and even jurisdiction) may be disguised or reported differently to their true location.

21. The issue is compounded when anonymising technologies are combined with encryption. Not only will the true location and identity of a user be obscured, but also their communications and online activities. Many of these technologies can be easily combined for cumulative effect, providing multiple layers of obfuscation, making it exceedingly difficult to attribute illicit activities to specific, identifiable offenders, and impeding the AFP's ability to effectively investigate serious criminality occurring online.

22. However, law enforcement are not alone in being challenged by anonymising and encrypted technologies. While moves to end-to-end encryption are promoted by companies as protecting user privacy, industry will be confronted by their own difficulties identifying criminal or malicious activity occurring on their own platforms, such as violent extremism or child abuse and exploitation. We anticipate this will challenge industry's ability to enforce user compliance with terms of service. For example, while platforms are taking steps to remove illegal or violent content from their platforms, the anonymity provided by these platforms to their own users means there may be limited opportunities for them to remove and detect repeat offenders.

Case Study #1

Inability to identify individuals due to anonymising technology prevented AFP from attributing criminal conduct

In a recent matter, the AFP investigated a sustained campaign involving dozens of emails sent to an individual in Australia, containing threats of violence and highly-offensive images. This conduct could constitute offences of using a carriage service to menace, harass or cause offence (contrary to section 474.17 of the Criminal Code) and using a carriage service to make a threat to kill (contrary to section 474.15 of the Criminal Code, punishable by maximum of ten years imprisonment).

The offenders used multiple anonymising technologies, including VPNs, re-mailer services and fake email addresses. This presented significant challenges to the investigation and despite exhausting all avenues of enquiry, the AFP was unable to identify the offender to attribute the criminal conduct to a specific individual.

This example demonstrates how the cumulative effect of anonymising technology can impact AFP investigations.

Criminal activity on the dark web

23. Over the last decade, the dark web has hosted an increasing number of large-scale, complex and anonymous platforms, services and marketplaces, where people can commit computer-related or enabled crimes with relative ease and anonymity. This includes producing and sharing child abuse material, purchasing illicit substances or firearms, procuring fake or stolen identities, conducting money-laundering and arranging other criminal activities (including murders).

24. These anonymising or hidden services and marketplaces are accessed using specialised software (including The Onion Router (TOR) and relays), and it is common for users to combine this with other anonymising or encrypted technologies, such as VPNs, allowing customers and vendors to remain anonymous.

25. Cryptocurrencies or digital currencies are often used for financial transactions, causing additional difficulties for investigators, as they can operate outside of centralised, regulated financial systems, and transactions do not need to be linked to a true identity.

26. For example, the illegal dark web marketplace 'Dark Market', which was taken down in January 2021 through combined international law enforcement efforts, sold drugs, forged currency, stolen or forged credit cards, anonymous SIM cards and malware. German prosecutors allege Dark Market had nearly half a million users, more than 2,400 vendors, had facilitated more than 320,000 transactions and exchanged nearly $AUD220 million in cryptocurrency.

27. Closer to home, in mid-2020, a Canberra woman allegedly attempted to hire a hitman via the dark web to murder her parents. This demonstrates the dark web's reputation as a place where wide ranges of illicit activities can be conducted or procured anonymously.

28. Despite international takedowns of well-known marketplaces, such as Silk Road (the self-styled 'eBay for drugs'), Hansa, AlphaBay and Dark Market, the ease with which users migrate to other platforms or establish new marketplaces if their preferred platform is taken down, means criminals are able to continue to sell and traffic illicit substances and

other illicit goods and services on the dark net, continuing the challenges for law enforcement agencies.

Impact on child protection investigations

29. The AFP is extremely concerned about the significant increase in child abuse material available for download on the dark web. The hosting, sharing and distribution of child abuse material is increasingly occurring on dark web (hidden) services, or through anonymising, encrypted messaging platforms.

30. The true picture about the amount of child abuse material facilitated by the dark web and anonymising technology is difficult to determine. While the ACCCE identified a significant increase in child abuse material downloaded on the dark web during April and June 2020, tentative estimates are that this represented less than half of the child abuse files available on the dark web.

31. The inherent anonymity offered by the dark web or anonymising and encrypted platforms, combined with the rise of live-streaming and pay-per-view services and the use of virtual currencies, makes it increasingly difficult to identify and track offenders. The true IP addresses, locations and jurisdictions of users and the services used, are usually hidden.

32. It is also common for criminal networks distributing child abuse material (including recordings of abuse) to take additional steps to hide their identity from law enforcement. For example, some services do not require payment to access; instead, users are required to produce and upload new child abuse material, to contribute to service content and gain access to restricted areas further up the network's hierarchy. Child abuse material uploaded or shared between users is usually scanned by the system administrators, to detect whether the child abuse material is being tracked (by law enforcement) or if it contains content which could otherwise reveal the location or identity of users or the host service.

33. These factors combined present substantial challenges for the AFP in identifying and locating perpetrators of abuse, and their victims, resulting in lengthy investigations. This also delays rescuing victims from harm and preventing the continuation of abuse.

Dedicated, encrypted communications platforms for the criminal market

34. Dedicated, encrypted communications platforms (i.e. using end-to-end encryption - a system of communication where only the users can see content) are increasingly being used and exploited by organised crime groups.

35. Australian law enforcement regularly encounter encrypted platforms when executing warrants on drug syndicates, outlaw motorcycle gangs (OMCGs), and other organised crime groups. These devices generally have common features, including:

    - only permitting encrypted communications (i.e. no regular phone calls, texts or web access) between other users on the same platform;
    - an ability to be remotely wiped; and
    - requiring expensive time-based subscriptions.

36. These features make it very difficult for AFP to access and uncover the identities of persons using these devices, and gain visibility of their criminal activities, even where a device is seized during a search warrant.

37. Infiltrating these encrypted platforms and devices through traditional law enforcement methods (i.e. search warrants and telecommunications interception) has proved largely ineffective, because these devices are generally being exclusively distributed only through known criminal associates, and users need to know the account name of those they wish to communicate with.

38. The exact nature and extent of offending facilitated through encrypted platforms often remains unknown until after the platform has been taken down in its entirety. This is because Australian laws do not allow the AFP to target identified encrypted platforms for intelligence purposes. Existing warrants require us to have first identified a particular person, or a particular handset, and also the specific offences that are being committed, before we can obtain a warrant. However, this information is often unavailable without a warrant to gain access to the platforms in the first place. This means the AFP currently has no reliable means to access this information.

39. This significantly undermines our ability to collect key information about a syndicate's activities at the early and evolving stages of their criminal planning, prohibiting us from proactively investigating broader offending, intercepting conduct before it escalates, and preventing its continuation.

40. The proposed new warrant powers in the SLAID Bill will help address some of these challenges and enhance the AFP's ability to proactively respond to serious cyber- enabled crime.

Use of dedicated encrypted platforms by organised crime

41. Some of these platforms are marketed directly to organised criminal groups, and have been used to facilitate a substantial level of criminality in Australia and abroad.

42. For example, in June 2020, European law enforcement took down the encrypted communications platform EncroChat, estimated to have over 60,000 users in 140 countries, who were engaged in extensive criminality.

    - In the Netherlands alone, access to the platform's contents led to the arrest of more than 100 suspects, the seizure of eight tonnes of cocaine, 1.2 tonnes of crystal methamphetamine, 20 million Euro in cash, dozens of automatic firearms, the discovery of 19 drug labs and the identification of facilities equipped for torture.

43. Through the actions of European law enforcement, the AFP was made aware that EncroChat also had a foothold in Australia's criminal community.

44. These examples demonstrate the continuing market for encrypted communications platforms designed exclusively for organised crime, and the serious offending which is facilitated without law enforcement visibility, and highlights the need for law enforcement to access these platforms.

AFP proposed use of new warrant powers

45. The SLAID Bill introduces three new powers, across the *Surveillance Devices Act 2004* (SD Act) and the *Crimes Act 1914* (Crimes Act) that will provide the AFP with additional, tailored warranted powers to enhance our ability to better protect the Australian community from serious cyber-enabled criminal activity.

Data disruption warrants – SD Act

46. The data disruption warrants in Schedule 1 will enable the AFP to **frustrate or stop the commission of serious offences** occurring online, by adding, copying, altering or deleting data held in computers. In practice, this means the AFP could covertly access computers to remove child abuse material, or alternatively deny access to computers or content, to prevent the continuation of serious criminal activity and minimise harm to victims, where traditional investigative action is not feasible.

47. It is important to clarify that data disruption warrants, while similarly worded, are for a completely different purpose to the computer access warrant and amended search warrant provisions introduced by the *Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA), which permit data modification only to facilitate evidence collection. These TOLA provisions were introduced to modernise law enforcement's electronic evidence-gathering powers, and to account for how our capabilities interact with electronic evidence, and do **not** permit disruption activities. Nothing in the SLAID Bill expands or otherwise affects the operation of those provisions. The Home Affairs Portfolio submission explains how the TOLA powers, such as computer access warrants, and the powers under the SLAID Bill interact in further detail.

AFP approach to disruption

48. While introducing an explicit disruption power is unique for Commonwealth law enforcement, it is also a logical extension of the AFP's existing, extensive disruption activity. The AFP already seeks to delay, divert or otherwise complicate the commission of criminal activity, or the operations of a criminal entity, to prevent or reduce crime-related harm in Australia. Enforcement, disruption and prevention are closely interrelated and complementary in fulfilling the AFP's objectives of protecting the community and causing maximum damage to the criminal environment.

49. Existing disruption efforts are typically a tailored response to a specific investigation or criminal threat, with the response reflecting the challenge at hand - especially if victims are at risk. Disruption may also be used numerous times and often occurs during investigations. However, it may also occur outside a specific investigation as a generic response to a crime.

50. Currently, the AFP innovatively uses a range of tactics and strategies including:

- traditional overt law enforcement powers, such as arresting and charging offenders to halt their activities, which will have the *effect* of disrupting a criminal plot (such as a planned terrorist attack or drug importation), or otherwise *damaging* the business model of a criminal enterprise (for example, through rescuing child abuse victims, and seizing the proceeds and instruments of crime);

- powers granted for the purpose of practical, preventative disruption; for example, terrorism control orders and preventative detention orders, and orders under the Proceeds of Crime Act 2002 to seize criminal proceeds and assets; and
- other powers or activities with an ancillary disruptive effect, such as inspecting an unregistered vehicle and discovering illicit drugs.

51. A successful disruption outcome may result in a significant increase in the risks and/or costs borne by an individual, group or network undertaking or participating in a criminal activity. These activities also create efficiencies by building relationships with partner agencies and reducing crime-related harm in Australia.

52. However, rapid changes in technology, and criminals' uptake of the dark web and anonymising technology, means traditional policing methods are not always the most effective method of addressing the threat posed by serious, cyber- enabled crime. Nor can we consistently rely on traditional policing methods to remove or minimise the immediate or enduring risk or harm.

53. Data disruption warrants will provide the AFP with additional tools to be proactive in targeting and frustrating serious offending. This will be particularly useful in situations where there are otherwise limited opportunities to identify, arrest and prosecute offenders, due to the lack of sufficient evidence or data to connect the offending to a specific location and/or individual. In this circumstance, the only option may be to take proactive disruptive action rather than investigative action, to prevent the continuation of the criminal activity.

Case Study #2

Use of data disruption warrants - Removing child abuse material and instructional material from dark web services

The hosting, sharing and distribution of child abuse material is increasingly occurring on dark web hidden services, which require specialised browsers, and other anonymising software, to access. Australian police work tirelessly to identify offenders who are producing, sharing and profiting from this vile material, and to identify and rescue victims. Some material uncovered by police can be extreme - depicting children, including very young children, being subjected to physical and sexual abuse, torture and cruelty.

Offenders are aware police are searching for them, so it is not uncommon for these hidden services to produce and share 'how to' guides on avoiding law enforcement detection, alongside instructional guides for producing child abuse material. The scale of membership is also alarming – many of these services have tens of thousands of users, all across the world.

Traditional law enforcement techniques struggle to address the scale of this problem. The **new data disruption warrants could assist to disrupt dissemination of child abuse material** on these hidden services, and **prevent ongoing collaboration by offenders**, through targeted action against hidden services when they are found by law enforcement (even if the precise identities of users or the location of servers has not been uncovered). The disturbing nature of the material distributed on these services justifies taking technical disruptive action. However, the type of action that is appropriate for police to take will depend on the available information in every unique circumstance.

Examples of technical disruptive action which could be considered under a **data disruption warrant** include deleting material which is available for access on a site (such as images or 'how to' guides), or complete disruption of access to the service, to ensure, as best as possible, that unidentified offenders can no longer access or distribute this material.

Case Study #3

Use of data disruption warrants – Disrupting criminal syndicates using malware to facilitate criminal activity

Between 2018 and 2020, the AFP investigated several complex malware syndicates operating via 'Botnets'. A Botnet can be described as a distributed network of computers infected by malware, which can be tasked by the malware syndicate to perform a variety of criminal activities, including banking fraud, ransomware and offensive cyber-attacks, amongst others. In many cases, the computers which form the Botnet belong to innocent people or companies, who are unaware their computers have been infected and are being used for criminal activities.

During these AFP investigations, in excess of 450,000 individual users were identified internationally as victims of these malware syndicates, including over 53,000 in Australia. Collectively, these victims lost an estimated $AUD 10 - 50 million.

At key points during these investigations, there were opportunities for police to systematically remediate computers infected by the malware (i.e. causing the malware to delete itself off victims' computers) to frustrate the ongoing commission of the offence harming Australians, while systematically remediating victims. However, Australian laws do not currently permit this sort of action – as computer access warrant powers are designed solely to facilitate evidence-gathering.

The new data disruption warrant will give the AFP another option to dismantle and disrupt these criminal syndicates by frustrating their offending. The AFP could alter the malware to reduce its reach and impact, disrupt malware infrastructure, while systematically remediating victims.

Case Study #4

Importance of providing law enforcement with disruption options to frustrate cybercrime syndicates using malware

Cybercrime costs the Australian economy approximately AUD$1 billion annually. Criminal use of malware is a significant problem impacting the Australian community. In 2020, Comparitech (an independent technology research company) reported that, on average, 11% of Australian computers, and 4.8% of Australian mobile devices, are infected with malware.

Internationally, malware infections have had devastating effects. For example, the global 'WannaCry' ransomware campaign in 2017 affected more than 200,000 computers in at least 100 countries. It crippled the UK National Health Service for several days, causing the cancellation of thousands of appointments and operations, at an estimated cost of £92 million pounds.

In the US, the 'Mirai' botnet, which targeted thousands of unsecured 'Internet of Things' devices, enabled cyber criminals to affect massive 'dedicated denial of service' across the US in 2016, impacting internet access for countless users. Even though Mirai's creators pleaded

guilty to various computer offences in 2018 after an FBI investigation, the source code for the botnet was released online, and it is still being used by criminals to facilitate offending.

The new data disruption warrant will create opportunities for law enforcement (including with the assistance of government partners) to better protect Australian victims through disrupting the ability of known criminal groups to operate their malware within Australia, and will be an effective tool to combat and remove threats in an expedient manner.

Network activity warrants – SD Act

54. The network activity warrants in Schedule 2 will allow the AFP to access data on computers used by criminal networks of individuals operating online, to collect intelligence about serious criminality including child abuse, violent extremism and trafficking illicit goods, to uncover who is involved and the scope of offending. By accessing the devices used by these groups over the life of the warrant, intelligence can be gathered that will allow the AFP to apply existing powers in a more targeted way, combatting criminal activity at the highest levels.

55. Collecting intelligence about criminal activity is vital to supporting the AFP's investigations and operational activities. Without technical and targeted intelligence collection powers, the AFP's ability to obtain the specific information required to take overt law enforcement action against offenders through arrest and prosecution is substantially diminished. Traditional intelligence and evidence collection methods, such as physical surveillance, location tracking, recording conversations and phone calls, and information from human sources, are not transferrable to online environments where all participants and transactions are anonymised and communications are heavily encrypted.

56. Information collected under a network activity warrant cannot be used as evidence; however, it can be used to inform the AFP's applications for evidence-gathering warrants, such as telecommunications interception, computer access and search warrants. It is the initial collection of this intelligence that will detect serious criminality, and provide sufficient information for the AFP to then precisely target and disrupt serious offending and maximise law enforcement's impact on criminal networks.

Case Study #5

Use of Network Activity Warrants - Targeting dedicated criminal communications

In 2018, joint efforts by the AFP, FBI and Royal Canadian Mounted Police (RCMP) resulted in the takedown of dedicated encrypted communications platform PhantomSecure, which was marketed directly to organised criminal groups and used to facilitate criminal activity in Australia and abroad.

In 2019, the PhantomSecure CEO was sentenced to nine years imprisonment in the USA in relation to racketeering offences for knowingly supplying encrypted smartphones to enable criminals worldwide to sell drugs, launder money and even organise murder. At the time of the CEO's arrest in March 2018, more than 10,000 Phantom Secure handsets were identified as in use in Australia. US court documents indicated these were being used by Australian outlaw motorcycle groups (OMCGs), including the Hells Angels, to organise several murders.

The new network activity warrants will allow the AFP and the ACIC to target criminal networks of unknown individuals who are using dedicated encrypted platforms (similar to

PhantomSecure), to collect intelligence through which particular persons, devices or offences can be identified.

For example, if network activity warrants had been available, the AFP could have more effectively targeted the PhantomSecure platform in Australia, including its use by unknown individuals for serious crime. This would have allowed the AFP to understand how the devices were used to facilitate criminal activity, identify the criminal suspects using these devices, and uncover the nature and scope of their offending.

The AFP and the ACIC could have used this intelligence to subsequently apply for evidence collecting warrants, including search and surveillance warrants. Overall, network activity warrants would have enhanced our ability to target organised crime groups, to reduce the trade in drugs and other illicit goods, and the perpetuating cycle of violence that is harming the Australian community.

Account takeover warrants – Crimes Act

57. The account takeover warrants in Schedule 3 will enable the AFP to seek a magistrate's authorisation to take exclusive control of a nominated person's specified online accounts, such as an account on a dark web forum, encrypted application, or social media, for the purpose of gathering evidence to further a criminal investigation.

58. The AFP has previously conducted account takeovers where the owner of the account has consented to AFP officers taking control of their account. The account takeover warrant will provide clear, legal authority to take over an account where the person does not provide consent, or it is not operationally viable to seek the person's consent (but where control of their account is necessary to gather evidence about serious criminal activity).

59. The ability to legally control a person's account will be a useful tool for investigators, particularly when used alongside existing powers, such as search warrants and controlled operations, or when investigators uncover additional accounts belonging to an offender after a search warrant has expired and the account could not otherwise be accessed without the account holder's consent.

60. Account takeovers are not intended to be exercised on their own – they are intended for use in conjunction with existing law enforcement powers (such as controlled operation provisions in Part IAB of the *Crimes Act 1914*), which each have their own thresholds, authorisations and robust oversight mechanisms.

Case Study #6

Use of account takeover warrants - Stolen Australian 'Remote Desktop Protocols' sold on dark web

The AFP investigated the sale of Remote Desktop Protocol (RDP) credentials on a dark web marketplace. The information being sold included usernames and passwords required to use a computer from a separate device, providing remote access. Use of stolen RDP credentials facilitates other crimes, including identity theft, fraud and use of ransomware. Unauthorised access to RDP has been assessed as a key driver to ransomware, which is the highest threat to Australian infrastructure at this time.

The dark web marketplace sold access to compromised RDP servers across the world. More than 10,000 Australian Internet Protocol (IP) addresses with RDP access were advertised for sale. Victim computers included residential home connections and Australian businesses.

The AFP identified numerous online accounts associated with a person allegedly responsible for the majority of purchases of Australian RDPs. These purchases gave the person a vast resource of stolen credentials, which could have been used to access the computers and servers across Australia.

When the AFP executed a search warrant, accompanied by a section 3LA Crimes Act order, and requested consent to take over his online accounts, the alleged offender initially refused to co-operate. He was arrested and charged for several cybercrime offences, including *unauthorised access, modification or impairment of data with intent to commit a serious offence* under section 477.1 of the *Criminal Code* (carrying a penalty of ten years imprisonment) and several counts of unauthorised access to restricted data. He was also charged for failing to comply with the 3LA order.

It took three months of negotiations through the courts before the offender complied with requests for his account details and consented to an account takeover. This was valuable time lost that could have helped identify victims and further offending. While the AFP charged the offender for failing to comply with the 3LA order, there is currently no recourse if an individual does not consent to an account take over.

If the AFP had the new **account takeover warrant**, we could have immediately assumed the offender's online persona to collect valuable evidence to prosecute Australian offenders engaging in cybercriminal activity, and in the course of doing so, determined the scope of stolen credentials available for sale. Where credentials aren't known, the AFP could obtain an assistance order, similar to a section 3LA order, requiring the offender provide any reasonable assistance, including account credentials and passwords.

Case Study #7

Operation BIRKS - Use of account takeover warrants - superannuation fraud facilitated by stolen Australian IDs available on the dark web

The AFP and the Australian Securities and Investments Commission (ASIC) have been jointly investigating a criminal syndicate which, since early 2018, has gained unauthorised access to Australian superannuation and share accounts, illegally withdrawing money from these accounts. This criminal activity was extensively facilitated by the dark web, and the offenders' use of anonymising, encrypted technology.

At this stage, one alleged offender has been arrested and charged. This matter is still before court, and investigations into the broader syndicate are ongoing.

The AFP alleges that once syndicate members gained access to a victim's superannuation account, they transferred funds to new bank accounts which were fraudulently created in other peoples' names using stolen identification documents. The funds were then used to purchase untraceable, physical assets overseas, which were then re-sold, with the profits distributed to syndicate members using cryptocurrencies.

As at September 2020, investigators believe more than AUD$5 million has been stolen, with more than AUD$14 million attempted stolen. More than 5,000 stolen and fraudulently-acquired identification documents have been used, and at least 17 Australian organisations were breached (i.e. personal identification was exfiltrated).

The syndicate bought and sold stolen identification documents through dark web marketplaces. Purchasing documents via the dark web allowed the syndicate to stockpile stolen IDs without any law enforcement oversight. Documents were also shared using an encrypted, cloud-based file-sharing application hosted overseas. Syndicate members also used pseudonyms on encrypted messaging applications to hide their identities.

The AFP has verified that other members of the syndicate are still actively acquiring and selling stolen Australian ID credentials on dark web marketplaces. We know that people overseas, including syndicate members, are making stolen Australian IDs available for purchase by people anywhere in the world.

Challenges faced in identifying criminal networks using online anonymising and other evasion techniques could be overcome more effectively if police could use the new Account Takeover Warrant to conduct overt or covert account takeovers.

If the AFP had identified the Australian offender's dark web accounts, we could have sought an **account takeover warrant** to gain access to criminal networks, to gather evidence of their true identities and locations and, in the course of doing so, gather insights into their broader activities.

Using the account of an existing syndicate member would enable AFP to use relationships of trust between syndicate members and/or marketplace users, against those same criminals. This could be more effective than trying to infiltrate a dark web forum as a new 'user'.

Case Study #8

Use of account takeover warrants - cybercrime investigations

In 2018, a foreign law enforcement agency referred information to the AFP about a website where paying subscribers could access stolen credentials of unknowing victims from around the world. The AFP investigation identified the offender who created and administered the site, and profited from the sale of the stolen identity information.

On 12 March 2019, the AFP executed a search warrant on the offender's residence and seized cryptocurrency and a laptop. During AFP examination of the seized material, a password manager was identified which contained 357 username:password pairs (used by the offender), for various online sites including chat messaging, financial services, cryptocurrency exchanges, infrastructure accounts, hacking, cracking and cybercrime forums, online storage and hosting sites.

If the AFP had been able to access and take control of these accounts via an **account takeover warrant**, we could have:

- Identified contacts, co-offenders and criminal associates, in Australia and elsewhere in the world from online forums supporting the offender's cyber-crime activity;
- Identified private messages (PMs) stored in online cybercrime forums, to evidence criminal intent and conduct;
- Identified funds (virtual and real) held in exchanges/wallets in jurisdictions where the AFP has no clear visibility (enabling opportunities to freeze funds);
- Identified infrastructure accounts to enable takedown or preservation of data for evidence; and
- Supported international law enforcement efforts to tackle cybercrime actors who operate on a global scale.

The new account takeover power would have been especially useful if the offender had administrator or privileged access rights, and would greatly assist in illuminating cybercrime networks operating in online forums.

Case Study #9

Use of account takeover power against dark web marketplaces

Operations against dark web marketplaces are time and resource-intensive, involving undercover infiltrations, combined with other technical capabilities, through which law enforcement seeks to uncover the identities and locations of customers, vendors, and the administrators (and their infrastructure) operating the marketplace.

Under current Commonwealth law, the AFP is constrained in its ability to take over a person's account. If the person does not consent, law enforcement has limited ability to take over and use that account, losing potentially valuable opportunities to gather evidence against dark web users and services which facilitate harm to the Australian community.

However, for foreign law enforcement agencies, account takeovers, used in conjunction with other traditional policing powers, have proven a useful tool when targeting these marketplaces.

Silk Road takedown - 2013

During the FBI's operation against Silk Road (the self-described 'eBay for drugs'), agents took control of a forum moderator's account, impersonating this Silk Road 'staff' member to establish trust with the marketplace's founder. This provided information that agents used to locate Silk Road's founder, Ross Ulbricht, and target Silk Road's platforms.

In December 2013, an Australian connection to Silk Road was uncovered when the AFP, in conjunction with the FBI, successfully located and arrested another Silk Road moderator, Peter Nash, as part of the international effort to take down the drug marketplace. Nash worked as a senior manager of a Forensic Disability Service in Brisbane, but was also earning US$1,000 per week to moderate the Silk Road forums (i.e. overseeing content). Nash was extradited to the United States and, in 2015, pleaded guilty to conspiracy to commit narcotics trafficking and money laundering. He maintained he never knew the identity of Silk Road's founder.

Nash's identity as a Silk Road moderator was only revealed after the FBI arrested Silk Road's founder, who had kept unencrypted identifying details of his 'employees'. If these details had been in encrypted communications, they would not have been found. It would have been more difficult for the AFP to identify any Australian connection.

If the AFP had been able to use the new **account takeover warrant** to takeover Nash's account, this could have facilitated collection of valuable evidence about Silk Road's operations, including (potentially) the location of the technical infrastructure supporting the market place.

Given a group of users attempted to re-start Silk Road for a number of months after the founder's arrest, control of an established moderator account such as Nash's could also have enabled the AFP to attempt to infiltrate the new group.

Hansa takedown - 2017

Hansa was one of several large dark web marketplaces which emerged in the wake of Silk Road, and account takeovers figured prominently in the international law enforcement response.

To facilitate the takedown, Dutch police took control of Hansa's critical 'administrator' accounts, after the men provided German police with their account credentials (following their arrest, for other offences, as part of a joint operation). Dutch police then impersonated the Hansa administrators for several weeks, gathering intelligence about the market's infrastructure, drug supplies and user base, obtaining data on more than 400,000 users.

This demonstrates the valuable intelligence and evidence which can be gained if police take control of existing accounts, particularly if the accounts belong to site administrators, or if the users have a trusted reputation.

Oversight and accountability

61. The AFP acknowledges that any expansion of law enforcement power requires robust oversight and accountability mechanisms.

62. The powers in the SLAID Bill can only be used by the AFP and the ACIC, and their application and use are strictly confined by the legislation. The powers can only be used where agencies reasonably suspect that serious criminal activity is occurring, meaning the offences under investigation must carry a penalty of three years' imprisonment or

more. These thresholds are consistent with other warrants in the *Surveillance Devices Act 2004* (Cth) (SD Act), and capture Commonwealth offences for possessing or sharing child abuse material, terrorism, trafficking drugs or weapons, and serious computer- related offences.

63. The new powers can only be used under warrant issued by a judge or AAT member (for data disruption warrants and network activity warrants) or a magistrate (for account takeover warrants), which is consistent with existing powers in the SD Act and the Crimes Act, and ensures that applications for the use of these powers are independently scrutinised.

64. The mechanisms in the SLAID Bill will ensure the AFP will be transparent and accountable in its use of these powers. The Commonwealth Ombudsman's oversight of data disruption and account takeover warrants is consistent with existing reporting for other SD Act warrants.

65. Noting their intelligence-gathering purpose, Inspector-General of Intelligence and Security (IGIS) oversight of network activity warrants will ensure the AFP's use of this power is justified, appropriate, and executed with due consideration to privacy and the rights of the Australian community.

Operational case studies to demonstrate use of all new warrant powers

66. The following additional case studies demonstrate how recent AFP investigations have been impacted by criminals' use of the dark web and/or encrypted anonymising technology, to the detriment of operational outcomes and the safety of the Australian community.

67. These examples also explore how each of the proposed new powers would have allowed alternative or complementary further action to be taken to progress or expand investigations into serious cyber-enabled crime, with often more successful outcomes.

Case Study #10

Operation DONABATE – Hypothetical use of all new powers to address use of encrypted communications by alleged terrorists

Operation Donabate was a Victorian Joint Counter-Terrorism Team (JCTT) investigation in 2018 into three radicalised men, who were inspired by extremist Islamic ideology and motivated to undertake violent jihad.

It is alleged the three men were planning to undertake a terrorist attack in Melbourne. The men were in the process of purchasing a firearm, allegedly with the intention of undertaking a large- scale attack, when police disrupted their plot in November 2018, by arresting and charging the men with other acts done in preparation for, or planning a terrorist act, which carries a maximum penalty of life imprisonment. The matter remains before court.

All three men previously had their Australian passports cancelled, after authorities became suspicious that they were intending to travel to a conflict zone. It is alleged that, because their ability to travel offshore was removed, the group changed approaches, and increased

communication using encrypted applications, to plan to undertake an act of politically-motivated violence within Australia.

The group used multiple encrypted communications platforms to conceal their activities. The group indicated they were aware that their communications could be monitored, which could potentially lead to them being questioned. They also showed concern about other online activities, such as accessing videos, recordings and other material that could have been monitored.

A **network activity warrant** would have allowed AFP to target all computers and devices used by the group over the life of the warrant, regardless of the group moving between multiple encrypted platforms to conceal their activities. This is because network activity warrants are not limited to gathering evidence from a specific computer network or device.

The group's use of encrypted communications meant it was difficult for police to decipher when and where the alleged plot was going to be carried out. The new **data disruption warrants** could have allowed police to frustrate the group's access to encrypted communications, disrupting their planning and making it easier for police to gather details about the plot.

The new **account takeover warrant** could also provide avenues to identify other offenders, to determine if they were part of a broader group, through taking over one of the identified offender's accounts, either to gather evidence or implement a covert engagement strategy (when used in conjunction with other policing powers, such as computer access warrants or controlled operations).

Case Study #11

Operation CEPHEUS – Hypothetical use of all new powers to address criminal distribution and use of malware

Operation Cepheus was an AFP investigation into the development and sale of the Imminent Monitor (IM) Remote Access Trojan (RAT).

IM RAT is a form of malware that requires little technical knowledge to use. It provides users the ability to remotely access documents, photographs and other files stored on a victim's device, record keystrokes and activate microphones and webcams, all without the victim's knowledge. Some of the Australian purchasers were known as respondents on domestic violence orders, and one was registered on the child sex offender register.

The malware cost as little as USD$25 and was sold on a well-known website dedicated to hacking and the use of criminal malware.

The AFP uncovered a distribution network, spanning 124 countries, which supported the sale and use of the IM RAT, with more than 14,500 recorded buyers.

In the first phase of action, cross-jurisdictional cooperation with Belgium (utilising the Budapest Convention on Cybercrime) enabled sharing of information and ultimately supported a successful prosecution of the co-accused.

The following phase involved a coordinated international 'week of action' by law enforcement in sixteen countries (coordinated with Europol and Eurojust) in November 2019. It involved 89 search warrants, resulting in 13 arrests and the seizure of 434 devices.

As a result of the search warrants, other serious crimes were identified and stopped, including computer misuse, fraud, dealing in proceeds of crime, narcotics and sexual offences.

In cases involving international cybercrime infrastructure, such as Operation Cepheus, very sensitive and complex capabilities may need to be deployed to identify and dismantle networks. This can result in lengthy, resource intensive and costly investigation periods.

The new powers, used in conjunction with existing legislation, will allow law enforcement to assume ownership of an identified actor's accounts (**account takeover warrants**), and/or disrupt the operation of their networks through use of technical capabilities (**data disruption warrants**), facilitated by the account access.

The new **network activity warrants** will also benefit future investigations like Operation Cepheus. Network activity warrants would have enabled police to identify the broader criminal network and gather intelligence more quickly. In turn, this would have allowed AFP to be more targeted in our use of evidence-gathering powers.