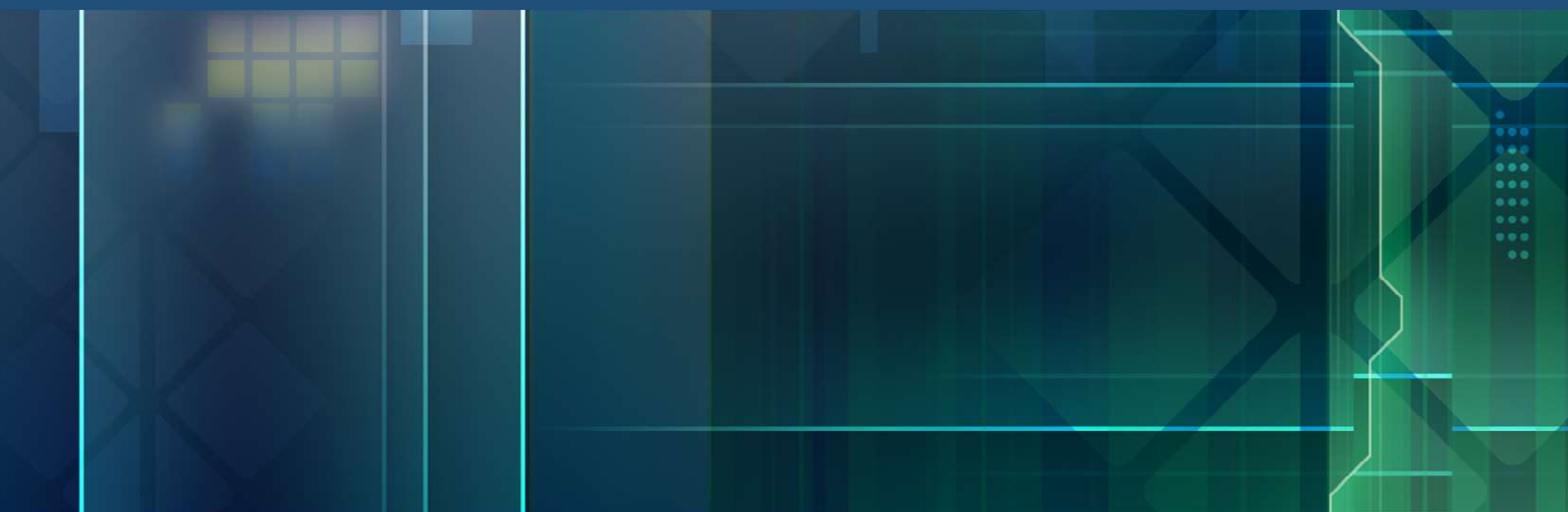
National Plan to Combat Cybercrime

2022



Contents

Ministerial Foreword / Executive Summary

The threats posed by cybercrime have significantly evolved since the release of Australia's 2013 National Plan to Combat Cybercrime. Advances in technology and the greater degree to which the Australian community utilises digital and communications technologies continue to increase opportunities for cybercriminals to take advantage of Australians and impact our security, public safety and prosperity. Cybercrime is not only growing in scale and sophistication, but cybercriminals are also becoming bolder in their activities and the targets they choose.

While increasing connectivity presents extensive economic and social benefits, the impact of cybercrime on Australia's society and economy is so significant that a national response is imperative. The Australian Cyber Security Centre (ACSC) *ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021* highlighted that self-reported losses due to cybercrime totalled more than AU$33 billion during the 2020–21 financial year. This is stark compared to the 2013 National Plan to Combat Cybercrime, which estimated the cost of cybercrime in Australia to be $2 billion annually.

And there are other immeasurable costs of cybercrime – no dollar value can reflect the immense harm caused to victims by all manner of cybercrime, such as the distribution of child abuse material, the spread of ransomware, or the compromise of personal information on a massive scale.

The COVID-19 pandemic significantly increased Australian dependence on the internet as it enabled working remotely, provision of access to services and current information, facilitated communication with friends and family and allowed Australians to continue their daily lives. Alongside the benefits of using the digital and online environment, vulnerability has rapidly increased as cybercrime networks capitalised on these social trends.

Cybercriminals adapt quickly to environmental changes and remain resilient to disruption by law enforcement. Cybercrime is a multifaceted threat, requiring multiple lines of effort to address it. Recognising the critical role state and territory law enforcement partners play in combating cybercrime, in cooperation with Commonwealth law enforcement, a nationally coordinated response is required to address the persistent challenge of cybercrime. Given the rapidly evolving nature of cybercrime, it is important that governments work closely with Australian businesses and the Australian community to empower them to remain vigilant and prepared as new cybercrime threats rapidly emerge.

It is therefore more important than ever before to implement a clear, strong and effective cybercrime framework for Australia, where Government, industry and the community work together to build Australia's resilience to cybercrime by fighting domestic and international cybercriminals and supporting victims of cybercrime.

This *National Plan* provides a unifying vision to support ongoing and evolving action to combat cybercrime. To this end, it builds on the actions of the Commonwealth, state and territory governments, including initiatives delivered under *Australia's Cyber Security Strategy 2020*, the *Ransomware Action Plan*, the *National Strategy to Prevent and Respond to Child Sexual Abuse* and the forthcoming *National Plan to End Violence against Women and Children*.

National Plan to Combat Cybercrime – Vision, approach and action

Vision

A secure, safe, just and prosperous online world for the Australian community, and a hostile environment for cybercriminals targeting Australians and their businesses.

Approach

This vision will be delivered through joint action by the Commonwealth, state and territory governments and meaningful engagement with industry, academia and the community. The National Plan to Combat Cybercrime (the National Plan) builds upon the strong foundations provided by *Australia's Cyber Security Strategy 2020*, the *National Strategy to Fight Transnational, Serious and Organised Crime*, the *Ransomware Action Plan*, the *National Strategy to Prevent and Respond to Child Sexual Abuse* and the forthcoming *National Plan to End Violence against Women and Children*.

Action

The National Plan to Combat Cybercrime focuses on three key pillars:

1. Prevent and protect
2. Investigate, disrupt and prosecute
3. Recover

The National Plan outlines the framework that further actions will be consolidated under, as part of the next phase of collaboration to combat cybercrime. This framework has been developed through extensive consultation with Commonwealth, state and territory stakeholders.

Consistent feedback received during this consultation period suggested an effective monitoring and evaluation mechanism was required to underpin the National Plan. The National Plan will drive outcomes through the establishment of the **National Cybercrime Forum**, consisting of all jurisdictions (including state and territory justice departments, Commonwealth, state and territory law enforcement agencies, and other regulators such as the Office of the eSafety Commissioner).

The Department of Home Affairs will lead the forum with the objective of developing the Cybercrime Action Plan that brings together the experience, powers, capabilities, experience and intelligence of all jurisdictions to build a strong multi-faceted response to cybercrime harming Australia and the Australian community.

The Cybercrime Threat

Cybercrime continues to pose a high threat to Australia's economic and social prosperity, causing wide ranging harms to its victims and broader society, including financial losses, emotional and psychological impacts, and the disruption of essential services. Cybercriminals are resilient, opportunistic and borderless. While cybercriminals are increasingly sophisticated in the way they pursue their illicit activities, advanced and anonymising technologies and darknet marketplaces also mean that less skilled actors can engage in cybercrime.

What is cybercrime?

Australia defines the term 'cybercrime' to describe both:

- **Cyber-dependent crimes** directed at computers or other information communications technologies (ICTs) (such as computer intrusions and denial of service attacks). These crimes did not exist prior to the introduction of computers.
- **Cyber-enabled crimes** (such as online fraud, identity crimes and child sexual exploitation and abuse), which can increase in their scale and/or reach through the use of computers, computer networks or other forms of ICTs.

Cyber-dependent crimes consist of conduct that only exists in the digital world, such as cybercriminals hacking networks to steal sensitive personal information or the use of malware (such as ransomware) to extort money from victims.

Cyber-enabled crimes are traditional crimes committed in new ways. Communications technologies, platforms and services (such as the internet) provide a pathway to commit crimes such as fraud, identity theft, trafficking in illicit goods, sexual abuse of children, and terrorism on an industrial scale.

Cybercriminals can range from individuals to criminal networks through to politically motivated actors. The motivations for cybercrime can vary significantly, including financial gain, interpersonal conflict, causing societal disruption, or gaining a competitive edge, through to being ideologically or politically motivated.

Example one: Ransomware and other cyber-dependent crime continues to grow

The ACSC assesses cyber-dependent crimes, such as ransomware, financial and other types of malware, and business email compromise, as significant threats facing Australia. The interconnectedness of our modern digital lives enables cyber-dependent attacks to impact systems that underpin the day-to-day functioning of society.

Ransomware is one of the most frequently used and damaging types of malware. It causes serious operational, financial and reputational harm to victims and can threaten the security of the broader community. It can affect any organisation, including businesses, educational facilities, hospitals and healthcare providers, government agencies, and non-profit entities. The ACSC Annual Cyber Threat Report assesses that ransomware has grown in impact and remains one of the most disruptive threats to Australian organisations. Almost 500 ransomware-related cybercrime reports were received via the ReportCyber website in the 2020-21 financial year, an increase of nearly 15 per cent over the previous financial year.

Example two: Impact of financial cybercrime

Online fraud and scams targeting Australia result in hundreds of millions of dollars funnelled into the pockets of cybercriminals every year. The proliferation of smartphones and the rise in social media, new payment technologies and online platforms have contributed to this growth, making it easier for cybercriminals to refine their strategies and engage with potential victims. Previously, it was common for scammers to engage with victims and persuade them to send money or personal identity information; however, now many scams involve limited contact with a victim, making it difficult for individuals to identify scam activity and take proactive steps to protect themselves.

Case study: Online scams against the Australian community

In 2021, the Australian Competition and Consumer Commission's (ACCC) Scamwatch received on average 700 scam reports with $870,000 lost each day. Further research commissioned by the ACCC in 2021 highlighted that 68% of people who encountered a scam did not report the scam. Based on these findings, and liaison with other organisations, ACCC expect the combined reported losses to scams in 2021 could be up to $2 billion. Due to significant underreporting of cybercrime, the true extent is likely to be considerably higher.

Example three: Cyber-enabled crime causes profound harm

State and territory police forces continue to adapt their cybercrime operations as traditional crimes such as drug trafficking move into the digital realm of darknet marketplaces. Illicit transactions are facilitated by anonymising technologies and cryptocurrencies, requiring specialised cybercrime investigation capabilities.

Case study: Law enforcement operations against darknet vendors

Strike Force VELLUM was an investigation by the NSW Police Force North West Region Enforcement Squad into a syndicate of offenders supplying prohibited drugs on the darknet. With the assistance of the NSW Police Force Cybercrime Squad, a controlled operation was conducted involving purchases of prohibited drugs using cryptocurrencies. Two offenders were subsequently charged with offences including large commercial supply and ongoing supply of prohibited drugs.

Other forms of cyber-enabled crime, such as technology-facilitated abuse and online child sexual abuse and exploitation, are a growing threat. AIC research[1] into women's experiences of Intimate Partner Violence (IPV) during the COVID-19 pandemic reports that one in 10 respondents (11.6%) had experienced some form of technology facilitated IPV by their current or most recent partner in the 12 months prior to the survey.

What is technology-facilitated abuse?

- abusive messages of calls
- account take-overs – accessing online accounts an preventing owner access)
- image-based abuse – sharing an intimate image without consent
- face social media accounts – harassing or negative commentary through social media platforms
- tracking an individual through a phone or device.

The Australian Centre to Counter Child Exploitation (ACCCE) has noted a significant increase in the amount of child abuse material downloaded since COVID-19 restrictions were implemented. Globally, there has been significant growth in certain forms of child sexual abuse, particularly livestreamed abuse, that operate entirely through cyber-enabled business models. The shift of contact offenders to online environments is likely to be a long-term trend that will continue to shape the threat landscape.

Case study: Significant increases in child sexual exploitation material

In 2020, the Australian Centre to Counter Child Exploitation reported that they received more than 21,000 reports of online child sexual exploitation. Each report contains images and videos of children being sexually assaulted or exploited for the sexual gratification of online child sex offenders.

1 ANROWS, 2021, Intimate Partner Violence during the COVID-19 Pandemic: A Survey of Women in Australia.

This online abuse is often linked to abuse in the physical world, with technology being used as an extension or enabler of violent and oppressive behaviours. Among women who experienced technology-facilitated violence, 73.5 per cent reported at least one type of physical violence, 48.8 per cent reporting sexual violence, and 94.5 per cent experiencing coercive control.

The eSafety Commissioner as Australia's independent regulator for online safety also continues to identify significant amounts of online abuse and harm.

Case study: eSafety complaints and reporting

The eSafety Commissioner administers a complaints system for illegal and harmful content under the Online Content Scheme as outlined in the Online Safety Act 2021. eSafety investigates reports and acts on material found to be 'prohibited or potentially prohibited', including child sexual abuse material (CSAM). eSafety prioritises reports about online child sexual abuse material and a single complaint to eSafety may lead to multiple regulatory investigations. During 2020–21, eSafety finalised investigations into 14,633 items of prohibited and potentially prohibited content, of which 98% met the definition of CSAM.

Australia's response to combating cybercrime

Strong foundations to combat cybercrime

Since the release of the 2013 National Plan to Combat Cybercrime, the Australian Government has implemented a number of measures to address the evolving threats posed by cybercrime, including:

- Passing the **Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (SLAID Act)** to enhance the ability of the Australian Criminal Intelligence Commission (ACIC) and AFP to discover, target, investigate and disrupt serious criminal activity occurring online.
- Signing the **Australia-United States CLOUD Act Agreement** under Australia's International Production Order framework, which will enable Commonwealth, state and territory law enforcement agencies and the Australian Security intelligence Organisation (ASIO) to obtain independently-authorised international production orders to facilitate timely disclosure of electronic data directly from communications service providers in the United States.
- Establishing the **Office of the eSafety Commissioner,** to help safeguard all Australians from online harms and to promote safer, more positive online experiences.
- Passing the **Online Safety Act 2021**, which places safety at the heart of how Australians navigate the online world by providing more powers for the eSafety Commissioner. The Act provides eSafety with strengthened powers to help protect Australians from the most serious forms of online harm. This includes enhanced information gathering powers to conduct investigations into specific online safety incidents through regulatory schemes, as well as new measures to improve broader online safety practices, transparency and accountability.
- Investing AU$1.67 billion over 10 years under **Australia's Cyber Security Strategy 2020**, to uplift Australia's cyber security baseline, delivering fit-for-purpose enforcement powers and capabilities to discover, target, investigate and disrupt cybercrime. This includes setting out the Government's approach to tackle the threat of ransomware through **the Ransomware Action Plan**, and AU$30.9 million invested over three years under the **National Cybercrime Capability Fund** to uplift the capability of Commonwealth and state and territory law enforcement agencies to combat cybercrime.

- Establishing the **ReportCyber** online reporting and referral system to allow members of the community to securely report cybercrimes to law enforcement for further investigation. ReportCyber also provides resources on other organisations that deal with specific types of cybercrime.
- Investing in **IDCARE cyber support services**, which provide specialist support to members of the community who have experienced identity theft, cybercrimes and scams that may result in financial or psychological harm. As part of *Australia's Cyber Security Strategy 2020*, the Australian Government has committed AU$6.1 million towards IDCARE to support Australians impacted as victims of cybercrime.
- Working collaboratively with industry to **protect the community from malicious SMS messages**, making regulations to give industry greater confidence to deploy their own capabilities to detect and block such threats.
- Establishing the role of Australia's Ambassador for Cyber Affairs and Critical Technology to represent Australia's interests internationally in cyberspace and critical technologies.
- Launching **Australia's International Cyber and Critical Technology Engagement Strategy 2021** which outlines how Australia will cooperate internationally across a range of cyber affairs. Under the Strategy Australia invests $AU74 million towards international cooperation initiatives to support our neighbours in Southeast Asia and the Pacific to strengthen their resilience, including specific projects to build capacity in cybercrime prevention and prosecution. These initiatives build on long-term efforts by the Australian Government to assist countries, including in the Pacific region to enhance their legal, policy and policing frameworks to strengthen capacity to combat cybercrime and online child sexual exploitation and abuse.
- Establishing the **Operation Orcus Taskforce**, coordinated by the Australian Federal Police, which brings together stakeholders from multiple government agencies across jurisdictions to combat the rising threat of ransomware in Australia and overseas.

Empowering government, Australian community and Australian businesses to combat cybercrime

Investigating criminal activity online is the responsibility of law enforcement agencies, including the **Australian Federal Police (AFP)** and **state and territory law enforcement agencies.** They are supported by the **Australian Criminal Intelligence Commission** and **AUSTRAC** through the provision of criminal and financial intelligence which enables law enforcement to investigate and disrupt cybercriminals. The **Commonwealth, and state and territory Directors of Public Prosecutions** are responsible for the prosecution of their corresponding Commonwealth and state and territory offences involving cybercrime.

The **Australian Competition and Consumer Commission** (ACCC) provides consumer protections to protect Australians and maintains *Scamwatch.gov.au*, which facilitates reporting of scams. The **Australian Communications and Media Authority** (ACMA) is responsible for the administration of unsolicited communications regulation and consumer safeguards in relation to telecommunications services. This includes regulation of telecommunications providers to identify, trace and prevent scam calls and actions to limit or prevent identity and financial theft perpetrated via telecommunications networks and services.

The eSafety Commissioner (eSafety) is responsible for ensuring Australians have safe online experiences by developing educational resources; administering reporting and takedown schemes for cyberbullying of children, cyber abuse of adults, image-based abuse and illegal and seriously harmful online content; and driving technological change through initiatives like Safety by Design and the Basic Online Safety Expectations Determination 2022.

The Department of **Home Affairs** leads the development of national cyber security and cybercrime policy. **The Australian Signals Directorate (ASD)** is the lead operational cyber security agency, with responsibilities spanning intelligence, cyber security and offensive operations against organised offshore cyber criminals to help mitigate serious cyber threat and strengthen defences.

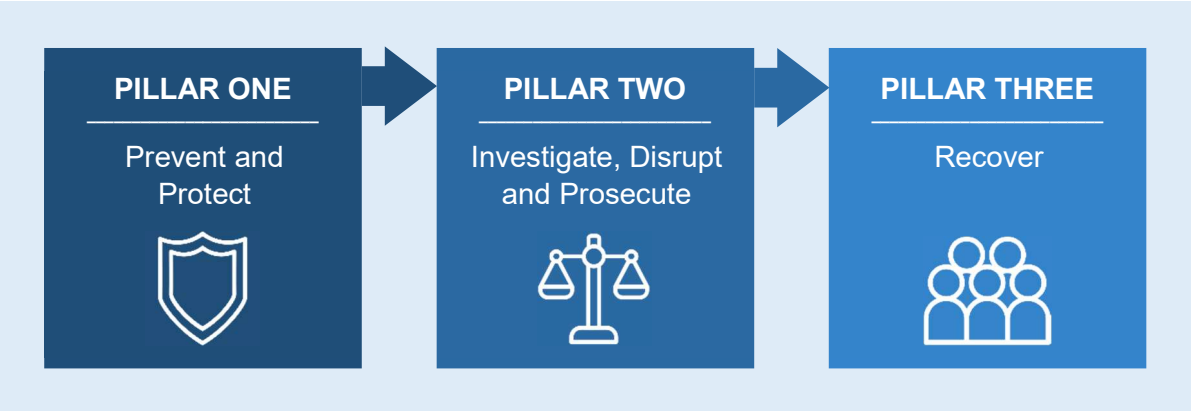
Internationally, **ASD** uses its offensive cyber capabilities to prevent and disrupt cybercrime conducted outside Australia. The **Department of Foreign Affairs and Trade (DFAT)** advances and protects Australia's international interests through enhancing diplomatic dialogue, cooperation and information sharing on cybercrime as well as strengthening regional resilience to combat cybercrime. DFAT also has a role in cybercrime attribution and deterrence framework for malicious cyber activities conducted offshore.

The Australian Government will continue to work with **industry**, including banks and communications providers. Industry continues to play an important role in disrupting and preventing cybercrime on their platforms and through the services that they provide. For example, following targeted consultation throughout 2021, the Government made new regulations to give telecommunications providers the confidence to deploy tools to block malicious SMS scams and protect their systems.

Key to all lines of efforts to combat cybercrime is the importance of empowering the Australian community to safely and confidently navigate the online world, allowing every day Australians to benefit from the digital economy. This includes ensuring Australians have the tools and knowledge to report and protect themselves from cybercrime.

The 2022 National Plan to Combat Cybercrime

A deliverable under *Australia's Cyber Security Strategy 2020*, the National Plan will build on the 2013 plan, taking into account the evolving cyber threat environment and the increasing dependence and reliance on cyber technologies. The National Plan will focus on three key pillars:



These pillars will ensure our national approach acknowledges the many facets of combating cybercrime across Australia.

Pillar One: Prevent and Protect

Preventing cybercrime is a high priority for the Commonwealth and state and territory governments. Building on strong foundations, all levels of government will leverage online safety and cyber security regimes to safeguard Australians, businesses, governments and our national security. Governments will work collaboratively with industry to sharpen Australia's ability to act flexibly and rapidly in responding to emerging cyber threats, which is crucial to minimising harms to our community.

Enhancing coordination across government will enable early engagement and response to cybercrime threats in line with the strategic objectives of the *National Strategy to Fight Transnational, Serious and Organised Crime, Australia's Cyber Security Strategy 2020* and the *International Cyber and Critical Technology Engagement Strategy*. Cross cutting efforts will also be delivered through the *National Plan to Prevent and Respond to Child Sexual Abuse* and the forthcoming *National Plan to End Violence against Women and Children*.

Action under this pillar will focus on:

- Strengthening Australia as a hostile environment for cybercriminals to ensure that they do not profit from targeting the Australian community.
- Supporting industry leadership to prevent and protect against cybercrime threats and consider how products and services can be made safer through security and safety by design concepts.
- Leveraging academia and Australia's cutting edge research and development to respond to the rapidly changing threat environment.
- Building confidence within the Australian community to improve their cyber security and safety habits to protect themselves from cybercrime threats.

- Working with international partners to enhance global responses to the threat of cybercrime, including through robust international frameworks that ensure our law enforcement agencies have the mechanisms and electronic evidence to investigate and prosecute cybercrime, while respecting human rights and the rule of law.
- Appropriately calling out those that willingly support or provide safe havens to cyber criminals.

These actions will build on successes to date as well as ongoing initiatives. Centralised coordination of national cybercrime priorities impacting Australian law enforcement agencies through national committees will remain critical to Australia's overall response to combating cybercrime. For example, the ongoing Operation HELIOS Joint Management Group and Operation ORCUS Taskforce will prevent cyber criminals from taking advantage of differences in jurisdictions.

Pillar Two: Investigate, Disrupt and Prosecute

This pillar recognises that strengthening criminal justice responses is key to ensuring law enforcement has the appropriate powers to investigate, disrupt and prosecute cybercrime. Enhancing coordination is critical to ensuring **consistency of national cybercrime legislation and criminal justice responses** of this pillar to counter malicious cyber actors.

The Australian Government is committed to delivering world leading legislative frameworks that keep pace with rapid technological and behavioural advancement. Legislative consistency across states and territories will also facilitate law enforcement interoperability. Action under this pillar will ensure law enforcement has investigatory powers frameworks that are fit-for-purpose, modern and future proof to respond to the evolution of technology. This will also ensure Australia's criminal offence framework for cybercrime is reflective of criminal misuse of the internet and other communication technologies.

Greater information sharing will be vital between public and private sectors to ensure that Australian law enforcement and prosecutorial bodies can effectively gather necessary evidence for investigations and undertake prosecutorial action against cybercriminals. A clear, data-driven national strategic and operational intelligence picture of cybercrime affecting Australia and Australians will be critical for ensuring law enforcement resources are allocated to targeting the highest harm and/or emerging cybercrime.

Global cooperation, including **through international forums remains essential** for strengthening global resilience to cybercrime. Australia leads by example, actively and constructively engaging in relevant international forums, including as a Party to the **Council of Europe Convention on Cybercrime (the Budapest Convention)**. The Budapest Convention is a fit-for-purpose and well-understood framework for international cooperation on cybercrime, with 66 State Parties and 12 observers.

Action under this pillar will focus on:

- Enhancing coordination across Commonwealth, state and territory law enforcement agencies, prosecutorial bodies, and other government agencies.
- Continuing to strengthen partnerships between public and private sectors to investigate, disrupt and prosecute cybercrime.
- Supporting law enforcement to access electronic evidence located in foreign jurisdictions to investigate and prosecute cybercrime and cybercriminals, which are often operating offshore.

- Ensuring law enforcement capabilities remain responsive to the rapid evolution of technologies, digital services and platforms.
- Delivering on government investments that have been made over the forward years to enhance Australia's capability to counter malicious cyber threats.
- Ensuring Australia's cybercrime legislation remains world leading and fit-for-purpose.
- Enhancing cybercrime data collection, reporting and intelligence which is imperative for understanding cybercrime threats and incidents impacting Australia.

Actions outlined under this pillar will be significantly boosted through the establishment of the AFP-coordinated **Joint Policing Cybercrime Coordination Centre** (JPC3). The JPC3 will bring together capabilities from across state and territory law enforcement, Commonwealth Government agencies and private sectors, to coordinate Australia's policing response to high volume cybercrime affecting the Australian community. The Centre will provide the platform to enhance collaboration between jurisdictional agencies, employing a compilation of unique skills, knowledge, tools and other resources to combat cybercrime and drive consistent and targeted efforts involving intelligence gathering, research, and the development of deterrence, prevention and disruption strategies and outcomes.

Pillar Three: Recover

This pillar recognises the significant impact cybercrime victimisation can have on Australians and their businesses, which is not only limited to financial losses. While empowering Australians to navigate the digital world is critical, so too is ensuring Australians can recover from a cybercrime incident. The National Plan recognises the importance of regularly examining feedback loops to keep victims better updated in relation to the progress of their matter following a cybercrime incident.

However, accurate and timely information on the nature, scope, scale and frequency of cybercrime activity is required to effectively combat cybercrime and support a holistic approach to prevention, response, recovery and resilience.

Action under this pillar will focus on:

- Continuing to build awareness among victims of cybercrime about how to access resources on recovery and how to report incidents, in partnership with law enforcement and the private sector to streamline access where possible.
- Continuing efforts between law enforcement and industry to stop illicit and fraudulent payment structures and processes.
- Reviewing post-incident feedback mechanisms to ensure feedback loops for cybercrime victims are as effective as possible.
- Continuing to support organisations specialising in post-incident support services; a commitment considered even more vital as cybercrime continues to evolve and impact more Australians and their businesses.

Working towards the future – The National Cybercrime Forum

Australia's continued uptake and integration of digital technologies and the increasing interconnectedness of online systems, particularly during the COVID-19 pandemic, has drastically expanded Australia's vulnerability to cybercrime. This has resulted in new opportunities for cybercriminals to target and exploit Australian businesses, critical infrastructure and individuals for profit, making cybercrime one of the fastest growing online harms and prolific forms of crime committed in Australia.

Implementing a clear, strong and effective cybercrime framework for Australia, where Government, industry, academia and the community can work together, will be key to strengthening Australia's ability to combat cybercrime.

Working in collaboration across the Commonwealth, state and territory governments as well as industry, academia and the community, we will:

- Strengthen Australia as a hostile environment for cybercriminals to ensure that they are unable to operate effectively against the Australian community.
- Support organisations specialising in post-incident support services and continue to build confidence within the Australian community to identify cybercrime threats and protect themselves.
- Continue to engage with international partners to respond to the threat of cybercrime.

Establishing the National Cybercrime Forum

The cybercrime threat is a national threat and Australia's successful response to combating cybercrime will rely on commitment to action from all governments. With this objective in mind, a National Cybercrime Forum will be established to bring together representatives from Commonwealth, state and territory justice departments, law enforcement agencies and regulators (such as the Office of the eSafety Commissioner) to develop the Cybercrime Action Plan.

The National Cybercrime Forum will be chaired by the Department of Home Affairs. In leading the forum, the Department of Home Affairs will leverage the experience, powers, capabilities, intelligence and experience of all jurisdictions to build a strong multi-faceted response to cybercrime harming Australia and the Australian community.

The Cybercrime Action Plan will outline detailed actions under each of the three pillars of the National Plan, as well as mechanisms for monitoring and reporting on implementation progress and outcomes.

The National Cybercrime Forum's Roadmap

- A secure, safe, just and prosperous online world for the Australian community, and a hostile environment for cybercriminals targeting Australians and their businesses.
- Strengthen Australia as a hostile environment for cybercriminals to ensure that they are unable to operate effectively against the Australian community.
- Support organisations specialising in post-incident support services and continue to build confidence within the Australian community to identify cybercrime threats and protect themselves.
- Continue to engage with international partners to respond to the threat of cybercrime.

Pillar One Prevent & Protect	Pillar Two Investigate, Disrupt, Prosecute	Pillar Three Recover
• Strengthening Australia as a hostile environment for cybercriminals to ensure that they do not profit from targeting the Australian community. • Supporting industry leadership to prevent and protect against cybercrime threats and consider how products and services can be made safer through security and safety by design concepts. • Building confidence within the Australian community to improve their cyber security and safety habits to protect themselves from cybercrime threats. • Continuing to work with international partners to enhance global responses to the threat of cybercrime, including through robust international frameworks that ensure our law enforcement agencies have the mechanisms and electronic evidence to investigate and prosecute cybercrime, while respecting human rights and the rule of law. • Appropriately calling out those that willingly support or provide safe havens to cyber criminals.	• Enhancing coordination across Commonwealth, state and territory law enforcement agencies, prosecutorial bodies, and other government agencies. • Continuing to strengthen partnerships between public and private sectors to investigate, disrupt and prosecute cybercrime. • Supporting law enforcement to access electronic evidence in foreign jurisdictions to investigate and prosecute cybercrime and criminals. • Ensuring law enforcement capabilities remain responsive to the rapid evolution of technologies, digital services and platforms. • Delivering on government investments over the forward years to enhance Australia's capability to counter malicious cyber threats. • Ensuring Australia's cybercrime legislation remains world leading and fit-for-purpose. • Enhancing cybercrime data collection, reporting and intelligence to better understanding cybercrime impacting Australia.	• Continuing to build awareness among victims of cybercrime about how to access resources on recovery and how to report incidents, in partnership with law enforcement and the private sector to streamline access where possible. • Continuing efforts between law enforcement and industry to stop illicit and fraudulent payment structures and processes. • Reviewing post-incident feedback mechanisms to ensure feedback loops for cybercrime victims are as effective as possible. • Continuing to support organisations specialising in post-incident support services; a commitment considered even more vital as cybercrime continues to evolve and impact more Australians and their businesses.

Government Action on the National Plan to Combat Cybercrime

The National Plan will bring together all jurisdictions to build a strong multi-faceted response to cybercrime harming Australia and Australians.

- Action: Establishing the National Cybercrime Forum, through the leadership of the Department of Home Affairs, to develop consolidated action plans under each pillar of the National Plan.
- Action: Engagement with state, territory and Commonwealth law enforcement and justice agencies.
- Action: Engagement with industry and academia to better protect the Australian community.
- Action: Monitoring, implementation and reporting to Ministers through the National Cybercrime Forum.
- Action: Ministerial level agreement to the National Plan.