Concept Paper

Countering CyberCrime:

A National Imperative

Submission

to the

Parliamentary Joint Committee on Law Enforcement

Inquiry into the impact of new and emerging information and communications technology (ICT) on law enforcement

14 January 2018

Countering CyberCrime: A National Imperative

Summary of Concept

Our dependence upon the Internet and cyberspace, as a universal vehicle for storing and manipulating information, for conducting business and for direct communications between individuals and entities, has created new vulnerabilities not only in the national security sphere, but also in terms of law and order. The Internet has become a ubiquitous new vector for old threats and old crimes.

Just as Cyberspace has become the Fifth Domain of Warfare, so Cybercrime is becoming one of the most profitable areas of criminal activity, impacting adversely on both individuals and the community as a whole. The global cost of cybercrime is expected to reach over $US 6 trillion in the early 2020s.

The Government is already implementing its comprehensive national Cyber Security Strategy announced in April 2016. While there are obvious linkages between the need to develop the greater cyber security resilience envisaged in that Strategy and the fight against cybercrime, this concept paper focuses on strengthening the national capability to detect, investigate and deter criminal activities conduct via Cyberspace.

Both national security threats and criminal activity exploit the Internet in similar ways. Both need to be countered or managed using similar investigative tools and techniques. Sophisticated cyber threats need to be countered with sophisticated cyber tools. Moreover, cyber tools facilitate the investigation not only of cybercrime *per se* but of a range of other crimes not necessarily committed over the vector of the Internet.

Australia’s national capacity to counter threats and criminal activity using cyber investigative tools is relatively under-developed, uncoordinated and fragmented across a range of agencies in both Commonwealth and State jurisdictions. This disaggregation makes it difficult for agencies to cope with the pace of technical change that is being taken up and exploited by those who would do us harm.

This Submission argues that countering cybercrime in Australia will be most effective when investigative support mechanisms are concentrated and coordinated on a cooperative national basis, utilising skills and technical capabilities developed in the national security area to strengthen law enforcement activity, and *vice versa*. National cooperative arrangements would constitute a critical mass of expertise able to operate on a scale that is too difficult and too expensive to achieve in a myriad of small under-resourced cybercrime capabilities spread around the country.

It therefore raises for consideration the concept of a single Commonwealth-led cooperative entity providing expert technical cyber investigative services in support of law enforcement and national security investigations carried out by Commonwealth and State agencies. It would support, rather that supplant or duplicate the proper functioning of those agencies under their existing legislative and operational authorisation requirements. It would also have a training and research function, to help develop the national capability to combat cybercrime.

Such an entity might fall within the policy ambit of the new Home Affairs Portfolio, but it would depend extensively upon the offensive and defensive cyber operational skills of the Australian Signals Directorate, and its offshoot the Australian Cyber Security Centre (which already operates cooperative arrangements in the cyber security area across Australia); and on law enforcement agencies for its practical operational focus. Academic centres of cyber security expertise and research, some of which already assist with investigative activities by law enforcement, might also be called upon to participate. Principal participating beneficiaries would include law enforcement and regulatory authorities from both Commonwealth and state jurisdictions, which might second staff into the cooperative arrangement

Countering CyberCrime: A National Imperative

Introduction: Old Crimes - New Technologies

Our dependence on the Internet and cyberspace as a universal vehicle for storing and managing information, conducting business and communications between individuals and entities has created new vulnerabilities affecting national security and law and order interests. The Internet is a ubiquitous new vector for old threats and old crimes.

Just as Cyberspace has become the Fifth Domain of Warfare, so Cybercrime is becoming one of the most profitable areas of criminal activity, impacting adversely on both individuals, institutions, businesses and the community generally.

The global cost of Cybercrime in 2017 is estimated at $US450 billion[1], rising to an estimated $US6 trillion by 2021[2] - larger than the GDP of any country outside of the United States and China and almost five times the current GDP of Australia. Estimates of the annual cost of cybercrime in Australia vary, but they are not insignificant. In 2016 the Attorney Generals Department estimated the annual cost of identity crime in Australia at $2.6 billion, with between 4% and 5% of Australians (approximately 1 million people) affected every year[3]. The Government's Cyber Security Strategy issued in April 2016 estimated the real impact of cybercrime to Australia could be as high as $17 billion annually.[4]

Malicious cyber activity extends from individuals abusing the Internet to express personal grievances or seek personal gain, to serious organised criminal activity and terrorist recruitment. It also extends to interference by Nation States in democratic processes or the operations of critical national systems**.** These are not new types of malicious activity. Rather, cyber technology is simply a new vector through which the traditional crimes of abuse, revenge, extortion, theft, sabotage and espionage are now being committed with relative impunity and immunity.

A key challenge is the speed of the development of offensive cyber technologies and the uses to which they are put for criminal activity. Those with malicious intent rapidly evolve techniques to exploit vulnerabilities in new technologies, using the latest digital obfuscation methods to hide their actions. Criminal activity and national security threats exploit cyberspace in similar ways; they therefore need to be countered and managed in similar ways – on a cooperative national basis.

[1] Hiscox Insurance Company

[2] Herjavec Group

[3] Attorney Generals Department *Identity Crime and Misuse Report 2016*

[4] Australian Government: *Australia's Cyber Security Strategy*, April 2016, P.15

Countering CyberCrime: A National Imperative

Part I - The Cyber Threat Phenomenon

Our growing dependence on the Cyberworld to regulate or facilitate almost every aspect of human endeavor creates vulnerabilities, which if not properly countered leave us increasingly open to both national security threats and criminal activity.

Cybercrime is transnational in nature. Cybercriminals and those responsible for national security threats do not respect traditional national borders. There are no hard cyber borders. Nor is there "cyber sovereignty" as espoused by some nations. The Internet is a global phenomenon, exploited globally with local, national and international consequences.

While they may differ in levels of sophistication, the basic tools of cybercrime are largely the same whether they are used by State or Non-State actors, or whether they pose threats to national security, our critical economic and social infrastructure or individuals, institutions or companies. These same basic systems and technologies are used to proselytise terrorist causes, conduct espionage or sabotage, promote subversive ideology, compromise and blackmail individuals and companies, groom minors for exploitation, disrupt democratic processes or steal classified data or Intellectual Property.

National Security Cyber Threats

The cyber vector may be exploited by both State and Non-State actors to pose three generic types of threat to national stability and security:

- **Espionage**: the theft of nationally sensitive information and data, including Intellectual Property, that can be exploited to our national disadvantage.

- **Sabotage**: disrupting or incapacitating warfare or defence capabilities; attacks that impact national resilience in both material ways (when directed at critical infrastructure)[5] and psychological ways.

[5] Critical infrastructure are those critical systems, services and facilities underpinning the operation of society and the economy, such as electricity and transportation networks, water services, healthcare systems and banking.

Countering CyberCrime: A National Imperative

- **Foreign Interference and Disinformation** to weaken our democratic institutions, national harmony, national resolve and national resilience.

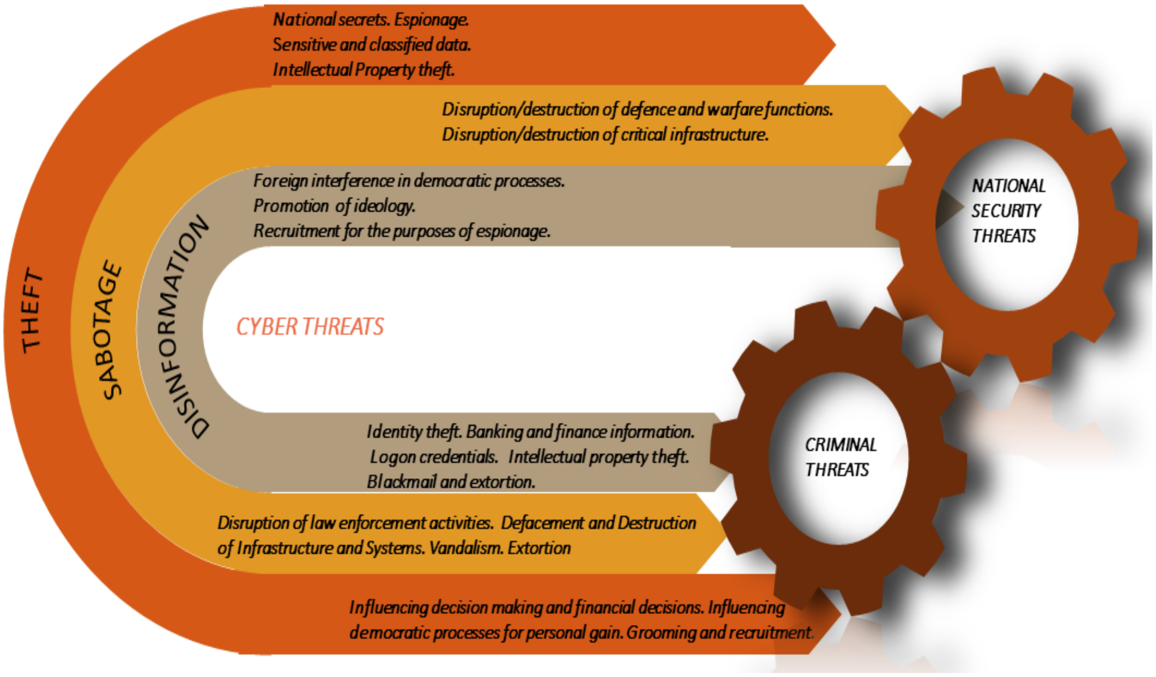
Cybercrime Threats

The cyber vector is also used to commit criminal offences, which broadly parallel the generic threats in the national security sector:

- **Information Theft**: the illegal acquisition of data of any kind that can be exploited for criminal gain, including theft of information related to identity, banking and finance, Intellectual Property, or legitimate computer system logon credentials.

- **Criminal Sabotage**: disruption or destruction of critical infrastructure, government services, law enforcement activities, commercial enterprises or personal devices to satisfy ideological or emotional needs or for financial gain.

- **Disinformation**: interference to affect the outcomes of democratic process in a way that benefits the perpetrator and disinformation campaigns that affect decisions and cause actions that otherwise may not be made.


National secrets. Espionage.
Sensitive and classified data.
Intellectual Property theft.
Disruption/destruction of defence and warfare functions.
Disruption/destruction of critical infrastructure.
Foreign interference in democratic processes.
Promotion of ideology.
Recruitment for the purposes of espionage.
NATIONAL SECURITY THREATS
THEFT
SABOTAGE
DISINFORMATION
CYBER THREATS
Identity theft. Banking and finance information.
Logon credentials. Intellectual property theft.
Blackmail and extortion.
CRIMINAL THREATS
Disruption of law enforcement activities. Defacement and Destruction of Infrastructure and Systems. Vandalism. Extortion
Influencing decision making and financial decisions. Influencing democratic processes for personal gain. Grooming and recruitment.

The Perpetrators

Perpetrators of Cybercrime range from individuals to companies, from lone hackers to organised crime groups, from terrorist cells to Nation States.

- **Nation States**: It is axiomatic that Nation States will seek to exploit the Internet in the service of their perceived national interests against those of other countries. Public accusation of such behavior has been levelled against countries such as North Korea, Iran, Russia, and China. In fact, covert use of the Internet for such purposes is likely to be more widespread.

- **Non-State Actors**: These can include Terrorists, Serious Organised Crime Syndicates, Single Issue Groups and individuals. The motivation behind cybercrime committed by individuals is varied: illicit financial gain, notoriety, personal grievance, recruiting and grooming people to commit acts of terrorism or to participate in human trafficking or child sexual abuse, etc.

Cybercrime Tools

Cybercrime tools, or vectors, include those technologies that collectively form the Internet, ranging from computers, mobile phones, CCTV cameras and the myriad of devices that are connected online, often referred to as the Internet of Things (IOT). The IOT includes such seemingly innocuous devices as televisions, printers, home security systems and refrigerators which often have weak security but permit access to the individual's or company's wider network. Within this environment cybercriminals deploy devices and applications that include:

- **Encryption and anonymisation tools** that hide the identity of the user by separating identity from online activity. An example of this is Tor[6], used by Dark Web websites such as AlphaBay to assist users in avoiding detection by law enforcement and intelligence agencies, as well as the social media and Internet service providers on whose backs they ride. Criminal use of uncrackable encrypted mobile phones has become a significant obstacle to effective law enforcement investigations.

- **The Dark Web, which** refers to that part of the Internet which is hidden from the view of typical search engines (e.g. Google, Yahoo, etc.). Its chief attraction

[6] Tor is free software that enables anonymous communication. Tor directs internet traffic through more than seven thousand relays to conceal the user's identity.

both to the criminals and the Nation States is the anonymity it offers to their communications. It can be accessed only with specific software, configurations or authorisations and which are also used by those with malicious cyber intent as another way to avoid detection. Dark Web communications are often used to facilitate cybercrime through Dark Web Markets (such as AlphaBay), where those using them can purchase stolen information (for example, credit card details, legitimate logon credentials for secure networks or identity information to be used for identity theft, as well as the ordering and acquisition of illicit goods such as drugs and weapons).

- **Dark Web Markets** also sell technologies including the latest hacking tools and even botnets for sale or hire. Botnets are 'zombie' computer networks of up to millions of compromised but legitimate devices connected to the Internet. By hiring a botnet those with malicious intent, regardless of who they are or what their grievance is, can launch a Distributed Denial of Service (DDoS) cyber-attack against any organisation connected to the Internet. For as little as $5 it is possible to hire enough botnet capability to block a large online store site for five minutes[7]**.**

Cybercrime tools can be tailored to achieve specific desired outcomes. Criminal organisations deploying ransomware as a form of cyber extortion will carefully select a price that makes paying the ransom attractive. The intent is not to make as much money as possible off one transaction but to build a business model that has a sustainable revenue stream. Ransomware can also be used for more sinister purposes, locking access to data in key social systems (such as hospitals, as happened in the UK in last year's *Wannacry* attack allegedly emanating from North Korea).

Nor do cyber-criminals always directly target the main entity of interest. If the main target has secure systems, it is sometimes easier to target and compromise a second entity which has a trusted relationship with the main target. This could include sub-contractors or other third parties with permitted access to the secure system. Through this abuse of the trust relationship, cyber criminals may introduce malicious software or tools into the main target's systems.

[7] Kaspersky Labs

Countering CyberCrime: A National Imperative

The Importance of Cyber Technology in Combatting All Forms of Crime

Criminal activity committed via Cyberspace usually requires both traditional law enforcement investigation techniques and cyber exploitation and investigation techniques.

While our dependence upon Cyberspace has created vulnerabilities that admit cyber-enabled criminal activity to our daily lives, Cyberspace has also created new tools for governments, law enforcement, and intelligence authorities to detect, investigate or disrupt vulnerabilities arising from criminal activity of all sorts – and not just cybercrime.

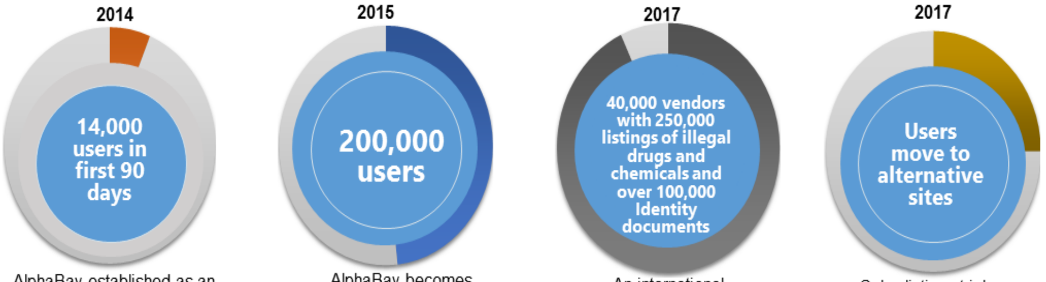
- **Data Exploitation**: Just as the major Internet and social media providers can exploit their customers' digital data for commercial gain, the exploitation of digital data held in Cyberspace is now a major investigative tool for law enforcement across all areas of criminal activity. That data may include such sources as social media sites, vehicle registration and vehicle movements, SCADA systems[8], CCTV, telecommunications data, financial transaction data and other forms of personal, commercial or business data.

- **Cyber Fingerprints**: The increasing use of cyber tools in the committing of crimes ultimately leaves digital fingerprints in Cyberspace. The intent of cyber-criminals is to hide their digital fingerprints through the Dark Web. Nevertheless, encryption or other anonymization tools leave some traces. Government, Law Enforcement and intelligence agencies need constantly to develop and exploit new tools to discover those hidden finger prints and traces if they are to counter cybercrime effectively.

- **Dark Web Exploitation**: Law enforcement and intelligence agencies need to understand and operate within the Dark Web if they are to conduct effective investigations into criminal activity or to protect the public against such activity.

[8] Supervisory Control and Data Acquisition systems. SCADA systems are often used to control critical infrastructure such as the flow of power and water.

Alphabay Dark Web Market: Case History



AlphaBay established as an anonymous darknet market for the exchange of illegal goods and services.

AlphaBay becomes the largest online darknet market.

An international operation led by the US Justice Department seizes and shuts down AlphaBay.

Sales listings triple on alternative Darknet site Dream Market as users shift platforms.

Part II –National Capabilities

There are two principal elements in the defence against attacks by cyber criminals:

- **Defence**: putting place appropriate protective systems and practices that can identify and repel or mitigate cyber attacks; and

- **Deterrence**: the ability of law enforcement to detect, investigate, disrupt and prosecute successfully acts of criminality conducted through the vector of cyberspace.

This concept paper focuses on the second of those elements: identifying, investigating and prosecuting cyber criminality.

Law enforcement agencies have long used elements of Cyberspace, including the information stored within it, to assist in criminal investigations. The use of telecommunications metadata and CCTV systems are well-understood examples.

A key challenge in the fight against criminal activity using the vector of Cyberspace is the ability of agencies to keep up with the rapidity and constancy of changes in cybercrime technology and the *modus operandi* of criminal activity. For example, the use of Ransomware as an extortion tool is estimated by one source to have increased 2000% in the last two years as the new generation of cyber criminals increasingly resemble traditional organised crime syndicates[9]

[9] Computer Weekly/Malwarebytes

Countering CyberCrime: A National Imperative

While it is true that outstanding work is being carried out by intelligence agencies and law enforcement teams across both Commonwealth and state jurisdictions, it is also true that Australia's emerging national capacity to cope with the pace of change and to counter threats and criminal activity conducted in Cyberspace remains under-developed, uncoordinated and dispersed.

There is a pressing need to maximise and build on current expertise dispersed around the country so that Australia is better prepared to face the challenge of countering the malicious misuse of cyber technology.

Commonwealth Cyber-relevant Entities

A range of Commonwealth agencies have cyber-related investigative requirements. These include those with direct responsibilities for cybercrime investigation, or cyber security advice and assistance, and those that use major cyber functions to inform their operations. Some of the principal agencies are detailed in Attachment A.

The increased use of cyber transactions between government and citizens means that most departments and agencies are likely to be targets of cyber-enabled crime. Those agencies with primary cybercrime investigation responsibilities will increasingly be required to assist other Government agencies in protecting themselves, their data and their client stakeholders.

States and Territories

There is also a range of state and territory entities, including jurisdictional police forces, with responsibilities for investigation of cybercrime. These entities should be encouraged to develop stronger cooperation between the jurisdictions and with the Commonwealth on issues related to cybercrime investigation and disruption, particularly as it is highly unlikely that volume cybercrime activity would be confined within the borders of a single state or national jurisdiction. While a level of cooperation has been achieved through the cyber unit of the Australian Criminal Intelligence Commission, there is not a lot of public evidence to show that this type of cooperation is as prevalent or effective as it could be.

State and local government entities may also be targets of cybercrime. State and local governments collect revenues, hold large volumes of personal data and manage critical infrastructure using SCADA systems.

Academic and Research Institutions

There are a number of academic institutions and research centres with cyber security capabilities, in addition to the Defence Science and Technology Group and the CSIRO's Data61. Moreover, specialist advice and assistance should be available from the private sector producers of technologies exploited by cyber criminals, and from academic centres of excellence in cyber security and cybercrime studies. These are potential non-government partners to assist law enforcement and intelligence agencies develop specialist knowledge to counter cyber criminals using new technologies.

Current State

Investigative cyber experts and counter-cybercrime capabilities exist within Australian state and federal government agencies, and parts of the academic community (including participants in the Cyber Security Research Centre).

By far the single biggest concentration of national cyber expertise lies within the Australian Signals Directorate, which hitherto has not played a particularly prominent role in countering cybercrime (outside of its use of cyber tools to support intelligence investigations into terrorism). If there is to be an effective cooperative national effort on cybercrime, the central role and expertise of the Australian Signals Directorate will be critical.

Other Commonwealth pockets of expertise include the Australian Federal Police, the Australian Criminal Intelligence Commission, the Australian Secret Intelligence Organisation, and the Australian Cyber Security Centre and CERT Australia (both currently focused predominantly on cyber security issues). State law enforcement agencies are also developing cyber investigative capabilities and skills; in the case of the Western Australian Police, in close collaboration with Edith Cowan University.

The national picture however remains one of fragmentation and disaggregation. Resources are scarce – in terms of funding and skilled personnel. There is a severe shortage of cyber experts and cyber-trained investigators within both government and industry.

This situation is exacerbated by the relentlessness speed with which the cyber environment evolves; cyber criminals have generally been able to adapt to this evolution and change tactics more quickly than investigative agencies. If not effectively countered, cybercrime will continue to become even more pervasive and public confidence in the efficacy of Australian law enforcement investigations and regulatory compliance measures will diminish. Failure to address cybercrime effectively will also lead to a loss of confidence for businesses operating online in Cyberspace.

Current Issues

- **Access to skilled staff**: There is a severe shortage of cyber expertise and cyber-trained investigators across both government and industry. This is a world-wide and not simply an Australian problem. Poaching of skilled staff is common, both within the public sector and by the private sector, with the private sector better placed to entice government-trained personnel away from government. For government, this constant churn means that recurrent expenditure on recruitment and training rarely achieves the desired forward momentum in enhancing effectiveness and productivity. The critical mass required to stabilize the labor market does not yet exist. Law enforcement agencies recognise the need to develop their cyber capabilities but are restricted by the availability of skilled staff and access to specialist training services for existing staff.

- **Disaggregated capability**: Technical cyber expertise within government tends to exist in only relatively small pockets outside of ASD – and ASD itself is challenged by the need to recruit and train appropriately killed cyber staff. These pockets are spread across a range of Commonwealth and State entities. There is a high cost associated with establishing and maintaining small, isolated cybercrime cells. There are reduced opportunities for isolated teams to share outcomes, learn from failings, share toolsets or develop cross agency awareness, not to mention sharing their expertise to assist in each other's investigations. Activity may be duplicated as separate teams strive to solve the same issues. Productivity is affected.

- **Research and training**: The ability to conduct research and provide specialist training is critical to developing a skilled operational law enforcement and intelligence capability against cybercrime. Some tertiary training research institutions offer advanced courses, and a few offer accredited higher level degrees, but it is difficult for government agencies to satisfy their exact training and education needs across the specialist options on offer by individual institutions. These services cannot be developed quickly or in isolation. A national approach to training in using cyber tools to fight cybercrime is required, including collaboration with private sector producers of technologies being misused by cyber criminals and with academic centres of excellence in cyber security and cybercrime studies.

Part III – Concept of a Cooperative Cybercrime Service Centre

The Cyber Intelligence Function

The Australian Government has need of a cyber intelligence function to support national security, national resilience and the efficient operation of the economy. This function is currently spread across a range of agencies including ASD, ASIO, AFP, ACIC, CERT Australia and the ACSC.

At the same time, there is also a need for specialist intelligence on the machinery, operation and use of cyberspace for cybercrime purposes, particularly given the speed with which the cyberspace environment evolves and the speed at which vulnerabilities in new technologies become subject to malicious misuse.

Cooperative Cybercrime Service Centre

The Cyber Security Research Centre considers there is merit in the concept of concentrating Australia's cybercrime fighting capabilities into a single national collaborative centre of excellence.

Purpose: The concept involves the creation of a Commonwealth-led national cooperative arrangement, which for the purposes of this concept paper we will call the Cooperative Cybercrime Service Centre (CCSC).

- It need not be a separate agency but could be set up within an existing agency. It would provide expert cybercrime investigative support services to government, national security and law enforcement agencies.

- It would have the capacity to conduct investigations and collect intelligence on cybercrime through the Dark Web. It would use its expertise to conduct the high-end cyber-related elements of law enforcement investigations on behalf of State and Commonwealth agencies.

- Client or participating agencies need not include only police or intelligence agencies. Other Commonwealth Government instrumentalities with some investigative requirements should also be able to draw upon the cyber investigative skills of the CSCC; for example, the border protection function involving immigration and customs, financial regulatory, taxation and social services functions, etc.

- Participating agencies would second expert cyber-investigative staff to contribute to investigations conducted by their parent agencies, leveraging common technical skillsets, methods and technologies concentrated in the CCSC.

Product: CCSC expertise should be drawn upon to contribute to **strategic assessments** on current and future trends in cybercrime, **operational assessments** related to particular spheres of cybercrime activity (e.g. the Dark Web, encrypted communications by drug dealers, pedophilia grooming activity, ransomware attacks and identity theft), and **tactical assessments** and direct support for specific investigative operations being conducted by participating agencies and jurisdictions.

Location: Given its law enforcement focus, the centre would logically come within the policy ambit of the new Home Affairs Portfolio. At the same time, by far and away the largest concentration of Australia's technical cyber expertise, including in encryption and offensive and defensive cyber capabilities, remains within ASD. It makes sense for that ASD capability to be exploited more comprehensively for the purposes of law enforcement against cybercrime. Given the centre's primary focus on fighting crime with cyber tools, law enforcement agencies would also need to be closely involved in its management and operation.

Concentration of Expertise: The CCSC concept should deliver economies of scale by concentrating specialist expertise and increasing productivity. It would espouse a culture of cross-agency knowledge and data sharing (as permitted by law). It would help to concentrate and focus the currently disaggregated and widely dispersed pockets of national expertise, with the long-term aim of establishing a critical mass of skilled cyber investigators able to assist investigative work across the national law enforcement spectrum.

Legislative Requirements: Investigative activities of the Centre would be governed by existing Commonwealth and state provisions regulating lawful intrusive access (for example, warrants, ministerial authorisations, the concept of investigative proportionality, etc.). Relevant Commonwealth legislation would include the Telecommunications (Interception and Access) Act, ASIO Act, Intelligence Services Act, Telecommunications Security Sector Reforms, Security of Critical Infrastructure Act 2017, the Customs Act (1901), Immigration Act (1901), Anti-Money Laundering and Counter-Terrorism Financing Act (2006), etc.

Legislative action to transform ASD into a statutory agency is contemplated. Legislation should make specific provision for ASD capabilities to be used to support criminal investigations by Australian law enforcement agencies and by relevant regulatory or administrative agencies (and specifically including investigations involving Australian citizens).

Role of Existing Agencies: The CCSC should not duplicate the roles of existing agencies. Responsibilities for cyber intelligence activities in the national security arena and for cyber security should remain with existing agencies in accordance with the Government's Cyber Security Strategy and national defence and intelligence policies.

- The CCSC would instead provide expert support services for both national security and law enforcement investigations and help develop national cyber resilience across the government, private and individual Internet-user sectors; in short, creating a strong national capability to fight crime of any sort where cyber investigative tools are required.

International Cooperation

A significant proportion of cybercrime affecting Australia originates from an international source. Cybercrime is a quintessential transnational form of crime and frequently must be fought as a transnational endeavor. As a result, law enforcement would need to cooperate with counterpart foreign cybercrime entities and law enforcement agencies. Wherever possible the work of the CCSC should leverage and strengthen international cooperation on countering cybercrime and increased cyber intelligence sharing. International cooperation presents an opportunity to increase knowledge and skills transfer between Australian authorities and trusted international partners.

Key Issues for Resolution

A number of key issues would need to be addressed in order to deliver a successful CCSC concept. These include:

- **Funding**: Agreement would be required on a funding or cost sharing model. Options may include direct funding by the managing Portfolio, by participating Commonwealth and state agencies or by funding on a fee-for-service basis – or a mix of each.

- **Inter-Agency Cooperation**: One of the key needs addressed by the recent structural changes involved in the establishment of the Home Affairs Portfolio was weaknesses in operational, intelligence and information sharing cooperation between the various agencies in the national security, border protection and national intelligence arenas. The CCSC concept should promote strong and effective cooperation across different jurisdictional and departmental authorities in the fight against cybercrime and other forms of crime.

- **Data Sharing**: A CCSC would work most effectively with instant access to all data relevant to cybercrime – with appropriate safeguards as to its proper (legal) use and distribution. Preferably access to data by the CCSC should be automatic, particularly given the way in which our cyber adversaries work quickly and do not respect jurisdictional boundaries. The CCSC would need to overcome any existing obstacles to data sharing between and within state and federal agencies. While the ultimate goal of government ought to be the harmonisation of data and privacy laws across Australia for intelligence and law enforcement purposes, the CCSC concept would still work within existing legislations.

- **Legal Confidentiality Issues**: Given different jurisdictional and legislative conditions across Australia, the CCSC would need to be able to conduct its investigative support activities in accordance with the legal requirements of the commissioning jurisdiction. Investigative legality and confidentiality, and the proper treatment of evidence, are key legal requirements for law enforcement activities aimed at achieving prosecutions. Where this were an issue, the problem could largely be resolved by having officers seconded to the CCSC from the commissioning jurisdiction conduct or manage the necessary cyber investigative activity, drawing upon the broader expertise of the CCSC, but applying their own specific jurisdictional investigative requirements.

- **Safeguards**: As with any law enforcement or intelligence activity, the CCSC would need to operate within the "ecosystem" of safeguards that protects the community against impropriety, abuse of process, unwarranted intrusiveness or any other unnecessary imposition upon civil liberties. This may not require new CCSC-specific legislation. The current "ecosystem" of safeguards and oversight governing the activities of both the Australian Federal Police and other investigative agencies and of the Australian Intelligence Community, together with relevant State legislation, would appear to offer appropriate protections for civil liberties and the rights of the individual.

- **Skills and Resources**: A major challenge for the CCSC concept remains that of obtaining and attracting qualified people to carry out cybercrime investigations and to master the Dark Web as an "area of operations". Much would depend on the willingness of Commonwealth, State and Territory jurisdictions to second suitable staff into the CCSC and to set salary scales that reward expertise. From the outset the proposed CCSC's mission should include the training and development of the skilled expertise necessary for an effective national cybercrime capability. This should include consideration of working with private sector producers of cyber technologies and with academic centres of excellence.

Conclusion

Countering cybercrime in Australia will be most effective when the mechanisms are coordinated on a national basis, using skills and technical capabilities developed in the national security area to strengthen law enforcement activity, and vice versa as the most effective means to deal with borderless crimes in cyberspace.

Choosing to proceed with the current funding and services is an option, however it is a high-risk decision based on what cyber security experts warn about the growth in global cybercrime, its increasingly coordinated and organised structure, and the speed at which new cybercrime techniques are identified and deployed.

Countering CyberCrime: A National Imperative

A new cooperative cybercrime security mechanism would assist Australia to develop stronger mechanisms and expertise to mitigate and protect us against the emerging threats posed by our increasing connectivity to and dependence on the Internet and cyberspace; in short, to secure our personal, corporate, political and economic wellbeing.

Appendix A: Government agencies with existing cybercrime and cyber security responsibilities and/or a requirement to protect major Government outcomes delivered online to benefit from CCSC

Agency	**Major roles/responsibilities related to cyber**
Australian Signals Directorate	Commonwealth authority on information security provides advice and assistance to Australian government agencies
*Australian Cyber Security Centre	The role of the ACSC is to: ▪ lead the Australian Government's operational response to cyber security incidents ▪ organise national cyber security operations and resources ▪ encourage and receive reporting of cyber security incidents ▪ raise awareness of the level of cyber threats to Australia ▪ study and investigate cyber threats.
Australian Secret Intelligence Service	ASIS undertakes counter-intelligence activities which protect Australia's interests and initiatives; and, engages other intelligence and security services overseas in Australia's national interests
Australian Federal Police	Investigates and responds to cybercrime of national significance. Part of the Department of Home Affairs and the Australian Cyber Security Centre
Australian Criminal Intelligence Commission	Discovers, understands and prioritises crime threat intelligence to enhance response options. Part of the Department of Home Affairs and the Australian Cyber Security Centre
Australian Security Intelligence Organisation	Responsible for issues related to cyber espionage in Australia. Part of the Department of Home Affairs and the Australian Cyber Security Centre
CERT Australia	The point of contact in government for cyber security issues affecting major Australian businesses, and within the global CERT community. Part of the Australian Cyber Security Centre
Department of Home Affairs	Includes functions performed by Border Protection Force, Department of Immigration, AFP, ASIO, Austrac and the Australian Criminal Intelligence Commission
AusTrac	Australia's financial intelligence unit, and the anti-money laundering and counter-terrorism financing regulator. Part of the Department of Home Affairs

Australian Digital Health Agency	Responsible for the digital health programme and responsible for the Digital Health Cyber Security Centre which strengthens the security of Australia's national digital health systems and services
Australian Taxation Office	Works to ensure a more secure cyber system to support Australia's system of taxation, and works with the Australian tax practitioner community to encourage a more secure cyber environment
Department of Social Services	Responsibility for families, housing, social services and disability services, much of which is delivered via cyber mechanisms
State and Territory law enforcement agencies	Jurisdictional law enforcement agencies with responsibilities within states and territories