Cybercrime to Cyberwar: Changing Strategic Perceptions of Cyber Security in Australia

Sara Delavere B.Arts, MRes.

Submitted 17 October 2019

Department of Security Studies and Criminology

Macquarie University

Contents

Tables

Abstract

Over the past 20 years, there have been significant changes in Australia's approach to cyber security policy. While information security had been a concern for Defence and industry across the late 20th century, the 2000 Defence White Paper was the first policy to address cyber crime as an issue for national security. Since 2000, cyber capability has taken a leading role, with both offensive and defensive cyber capability at the forefront of Australia's long-term defence planning.

Drawing on an analysis of Australia's publicly available Federal Government policies, this thesis argues that between 2000 and 2019 there has been a major shift in discourses around cyber security, from that of a policing framework, to a national security framework. Furthermore, this thesis argues that these discourses actively shape law enforcement responses to cyber threats across both industry and government. This is demonstrated through a comparative analysis of two case studies, the Joint Banking and Finance Sector Investigations Team of 2004 and the Joint Cyber Security Centre initiative of 2018.

Statement of Originality

This work has not previously been submitted for a degree or diploma in any university. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

Signed: Date: 17 October 2019

Sara Delavere

Acknowledgements

This thesis would not have been possible without the support of my family and friends, who have listened to my cyber policy rants for the past 10 months. Thank you for your love and support and for the endless supply of chocolate!

Thank you to my supervisors Allon and Stephen for your help and guidance across this thesis year, and for always being up for a discussion.

1. Introduction

Over the past 20 years, there have been significant changes in Australia's defence policy, particularly in relation to the role and importance of cyber security. The 2000 Defence White Paper presented the first plan for how Australia would manage the opportunities and challenges facilitated by the development of new technologies in cyberspace. This has remained a concern across federal policy documents, with cyber capability taking on more of a leading role, with both offensive and defensive cyber capability at the forefront of Australia's long-term defence planning.

This thesis argues that between 2000 and 2019 there has been a major shift in discourses around cyber security, from that of a policing framework, to a national security framework. Furthermore, these discourses actively shape law enforcement responses to cyber threats across both industry and government. I will begin with an analysis of publicly available Australian Federal Government policies between 2000 and 2019 to show how discourses around cyber security have changed. Then, I will present a comparative analysis of two case studies; the Joint Banking and Finance Sector Investigations Team of 2004 and the Joint Cyber Security Centre initiative of 2018.

The Joint Banking and Finance Sector Investigations Team (JBFSIT) was created in 2004 by the Australian High Tech Crime Commission in response to a rise in electronic crime targeting financial information. The JBFSIT brought together expertise from the Australian Federal Police and the banking sector to collaborate and find ways to address the rise in financial fraud. The Joint Cyber Security Centre (JCSC) initiative was announced as part of the *2016 Cyber Security Strategy*. The JCSC initiative was designed to be a collaboration between industry, government and law enforcement to facilitate information sharing and threat analysis in the face of the rising threat of cyber-attacks across the critical infrastructure and national security sectors. These case studies will demonstrate that the discursive shift across Government policies also has an impact for both the private and public sectors in the responses to cyber threats.

There is little research on this topic, particularly in an Australian context. This thesis exposes a gap in the existing literature and will examine the ways that Australia's cyber security

strategic priorities have evolved, and the impact this has on both law enforcement and private industry. This thesis speaks to a broader post-9/11 shift and a rise of non-traditional threats in contemporary Western society, as well as technological developments leading to an increased integration of digital technologies into everyday life, and an increasing reliance on the digital economy and the new threats posed by this integration.

1.1 Literature Review

Over the past 20 years, there have been major shifts in Australia's cyber security policy, starting from the 1994 Defence White Paper, to the 2017 Independent Intelligence Review. This literature review will first discuss the two case studies discussed in this thesis, the Joint Banking and Finance Sector Investigations Team (JBFSIT) and the Joint Cyber Security Centre initiative (JCSC) in terms of the academic and government literature available. It will then discuss the existing literature on Australia's cyber security policy and approaches and demonstrate the lack of literature addressing the shift from cyber security as cybercrime prevention to national security focused. Furthermore, this literature review will argue that the gap in the literature is not exclusively Australian by discussing the literature available on national security and cyber security.

1.1.1 Cyber Security and National Security

There is a growing body of literature discussing the connection between cyber security and national security. *Cybersecurity and Cyberwar: What Everyone Needs to Know* by Singer and Friedman (2014) provide an accessible and informative analysis of the importance of cyber security and modern issues facing governments and the general public. Their discussions are most applicable to Western Liberal Democracies with much of the discussion centred around the United States, but they do discuss the attitudes around cyber warfare of different states including China (Singer and Friedman 2014). However, while Singer and Friedman (2014) discuss a range of contemporary cyber issues, including national security and cyber warfare, hacktivism and state-sponsored cyber activity they do not discuss how cyber security came to be considered a national security concern (Singer and Friedman 2014).

Comparatively, *Cyberspace and National Security* edited by Reveron (2012) provides a more focused analysis of the relationship between cyberspace, state interests and national security, with an examination of the United States, Russia and China. They explore the history of the United States' integration of cyber capability and computer crime capability into their national security framework (Reveron, 2012). Both Reveron (2012) and Singer and Friedman (2014) focus on global powers, particularly the United States. There are also a lot of discussion about cyber warfare and the role of cyber capability in international relations, and how cyber warfare and information warfare can be used to achieve state objectives (Shakarian et al., 2013). In particular there are bodies of literature that discuss how China and Russia capitalise on the opportunities afforded by cyber capability and information warfare (Reveron, 2012, Austin, 2018).

In addition, there is also a large body of literature on the role and importance of public-private partnerships (PPPs), particularly in relation to critical infrastructure protection (see for example Givens and Bush, 2013, Hare, 2009 and Morag, 2011). Carr (2016) provides a comparative analysis of private and public sector responsibilities and attitudes towards critical infrastructure protection in the United States and the United Kingdom. Dunn-Cavelty and Suter (2009) argue that while public-private partnerships can be extremely beneficial for all parties, without clear boundaries and communication, public-private partnerships will not perform the required function for either party. Koski (2015) applies this idea to the United States, arguing that the success of public-private partnerships between the Department of Homeland Security and industry partners in the United States is based on the key factors of trust, goal tracking, organisational culture awareness and partnership planning based on common goals. Without these key factors, the public-private partnerships do not fulfil the needs of either partner (Koski, 2015).

1.1.2 International Perspectives on Cyber Security

Cyber security policy is a growing field, with research undertaken both about cyber security in general, and specialised literature on the cyber security policy of different nation-states. For example, Bayuk et al.'s (2012) *Cyber Security Policy Guidebook* provides a comprehensive overview of the relationship between technology, security, cyber and government in order to discuss the important elements of cyber security policy.

There is also state-specific literature that examines in depth how different states integrate cyber-based concerns into their national security policies and cyber security strategies. For example, Ventre's *Cyber Conflict: Competing National Perspectives* contrasts the evolution of and attitudes towards cyber capability in cyber security policies across the world including Greece (Fitsanakis, 2012) and South Africa (van Niekerk and Maharaj, 2012). Luiijf, de Graaf and Besseling (2013) examine the cyber security strategies of 19 countries of different sizes, comparing their approaches to and priorities within their cyber security strategies. Loiseau and Lemay (2012) discuss the major influencing factors in Canada's cyber security policy, providing both a history and analysis. In addition, there is literature about the European Union and cyber security (see for example Ruohonen et al., 2016 and Christou, 2016).

There is also a large body of literature on Cyber Security in Western liberal democracies, especially the Five Eyes partners (see for example Malone and Malone, 2013, Lonsdale, 2016 and Burton, 2013). This ranges from that discussed above in public-private partnerships (Carr, 2016, Koski, 2015, Clinton, 2015) and the connection between cyber security and national security (Reveron, 2012, Singer and Friedman, 2014). Kaplan (2016) traces the development of the United States' cyber security awareness, placing the first considerations of cyber capability in 1983. He argues that this early awareness shaped the United States' responses and policy directions, giving them an early awareness (Kaplan, 2016). Sanger's (2018) *The Perfect Weapon* explores cyber warfare and the role of cyber capability in modern society designed for general consumption, focusing on the United States. Flowers and Zeadally (2014) compare the cyber defence policies of the Unites States to those of other Western countries, to assess the risks associated with active defence policies.

1.1.3 Academic Research on Australia's Cyber Security

There is little academic research on the trajectory of Australia's cyber security policy. Smith and Ingram's 2017 paper 'Organising Cyber Security in Australia and Beyond' provides a comprehensive history of Australia's cyber security infrastructure, focusing on private and public engagement with the CERT model, or Computer Emergency Response Team model (Smith and Ingram, 2017). They discuss the reluctance of the Australian federal government to invest resources in cyber security, and the innovation from the private sector at the University of Queensland, Griffith University and the Queensland University of Technology

leading to the creation of AusCERT. (Smith & Ingram, 2017). AusCERT's key priorities related to threat monitoring and analysis, educational resources on threat mitigation and recovering from cyber-attacks, and communicating with national and international partners on sensitive cyber issues (Smith & Ingram, 2017: 646). Smith and Ingram's research is based on government websites (many of which are not accessible in 2019), government documents, as well as interviews and documents from private archives (Smith & Ingram, 2017).

Warren and Leitch (2011) examine the Federal Government's approach to critical infrastructure protection, analysing Government approaches and policies, and discuss how critical infrastructure ownership has changed over time and the impact of this on government policy. Warren and Leitch (2018) also compare Australia's 2016 Cyber Security Strategy (2016) and the Cyber Security Strategy Framework from the European Union Agency for Network and Information Security. They note that while Australia meets 87% of the criteria, there are areas in which improvement needs to be prioritised such as providing consumers with information on the safest technologies to use, which helps create a cyber-aware population (Warren and Leitch, 2018). Warren and Leitch also note that a key difference between the European Union's approach and Australia's in the role of the Australian Cyber Security Centre in combining military and civilian cyber intelligence and advice (Warren and Leitch, 2018).

There is literature from both academia and organisations such as the Australian Strategic Policy Institute (MacGibbon, 2009, Jennings and Feakin, 2013) and the Centre for Defence and Strategic Studies (Brookes, 2015) discussing specific policies and papers released by the Federal Government. For example, Slocombe (2013) examines the 2013 Defence White Paper's cyber security measures, discussing how the attitude to cyber capability has changed since the 2009 Defence White Paper. Furthermore, Slocombe (2013) discusses the shortcomings of the 2013 Defence White Paper in terms of the lack of operational and strategic planning for how to achieve the Government's goals.

1.1.4 The Joint Banking and Finance Sector Investigations Team 2004

The Joint Banking and Finance Sector Investigations Team (JBFSIT) was created in 2004 by the Australian High Tech Crime Commission in response to a rise in electronic crime

targeting financial information (Platypus, 2009). It was a public-private partnership (PPP) comprised of staff from the AFP and the banking sector on secondments (Platypus, 2009).

The JBFSIT continued through to 2009 and was an influencing factor in the formation of the Australian Identity Fraud Protection Register, also established in 2004 (Platypus, 2009, McKenzie, 2006, Jamieson et. al, 2009). The JBFSIT was considered a success, leading to increased collaboration between competing banks and information and intelligence that led to successful investigations and prosecutions by the Australian Federal Police (AFP) (McKenzie, 2006, Platypus, 2009, Parliament of Australia, 2007). There are two competing views on the biggest success of the JBFSIT; first, that the success was a product of the secondment arrangement between the banking sector and the AFP (McKenzie, 2006). The second argument credits the success of the JBFSIT in the collaborative relationship between the banking sector and the AFP, then later expanding to include collaborations with other government agencies (Burge, 2009, Jamieson et. al, 2009).

The JBFSIT and its efficacy has been examined through reports published by the Australian federal government including the Report of the Inquiry into Cybercrime of 2010. This report explored the impact of the JBFSIT and the evolution of other initiatives to combat cybercrime that emerged out of this task force (Parliament of Australia, 2010). Again, the enduring success of the JBFSIT is credited to the collaborative arrangement between the AFP and the banking sector (Parliament of Australia, 2010). The Senate Legal and Constitutional Legislation Committee of the Attorney-General's Department identified the key piece of legislation for the JBFSIT as the *Cybercrime Act of 2001*, which was the first comprehensive pieces of legislation for prosecuting cybercrime (Williams, 2006, Cybercrime Act, 2001). Furthermore, the Senate Standing Committee on Legal and Constitutional Affairs: Australian Federal Police of 2007 summarises the statistics for investigations and their success between 2004 and 2007 (Parliament of Australia, 2007). This document outlines the number of investigations, referrals and successful prosecutions of the JBFSIT and further emphasises the importance of the JBFSIT (Parliament of Australia, 2007).

McKenzie (2006) argues that the key flaw in the JBFSIT was the difference in perspective of secondment length of the staff between the banks and the AFP and AHTCC (McKenzie, 2006). While predominantly comprised of personnel from both the AFP and the banking sector, there was no agreed length of secondments (McKenzie, 2006). Personnel were allocated by the banking sector based on their perceptions of the needs of the JBFSIT, leading

to much shorter secondments than the AFP (McKenzie, 2006). Given the high training time for each staff member, the shorter secondments led to a waste of resources in repeatedly training new staff and then losing their expertise before it could be leveraged (McKenzie, 2006). In contrast, the Platypus magazine edition 103 cites the key challenges faced by the AFP and their partners as the transnational and border crossing nature of electronic crime (Platypus, 2009, Burge, 2009). The difference in proposed reasons for success may arise from McKenzie's PhD focusing on public-private partnerships (PPPs) at a state level, evaluating their efficacy in meeting both the needs of the public and those of the private partner (McKenzie, 2006). He also discusses the PPPs in terms of the potential for corruption from individuals in the form of preferential treatment and recommendations for allocating contracts based on kickbacks and monetary gain (McKenzie, 2006).

1.1.5 The Joint Cyber Security Centre Initiative 2017-2018

The first of the Joint Cyber Security Centres (JCSCs) opened in Brisbane in February 2017 as a part of the Australian Government's 2016 Cyber Security Strategy (Department of the Prime Minister and Cabinet, 2016).The JCSCs are designed to be a site of collaboration between industry, government and law enforcement to facilitate information sharing and threat analysis, with each partner providing resources to the centre (Australian Government, 2017).

The Australian Government's Australia's Cyber Security Strategy: First Annual Update (2017) identifies the JCSCs as the point of collaboration for industry, law enforcement and government (Attorney-General's Department, 2018). This report identifies the priority of the JCSC as information sharing and threat analysis (Australian Government, 2017). The JCSC initiative has an extensive and diverse list of partners including major retailers, Australian universities, state and federal government departments, banks, utilities providers and airlines as well as smaller businesses (Australian Signals Directorate, 2019c). The large partner list (Australian Signals Directorate, 2019c) and the variety of industries present demonstrates the importance and impact of the JCSC.

There is little academic research on the Joint Cyber Security Centre. This may be because it is still in its infancy, with locations opened between the 2017 and 2018. It may also be due to the arrangements that the JCSC have with the participants, with each partner organisation

required to sign a Deed of Confidentiality (CERT Australia, 2018). Finally, the lack of academic research may also be due to the close relationship between the JCSC initiative's parent organisation the Australian Cyber Security Centre (ACSC) and the Australian intelligence community, particularly the Australian Signals Directorate (ASD).

Information on the JCSC can predominantly be found on the current ACSC website (ACSC, 2019), CERT Australia (Australian Signals Directorate, 2019b) website and the still under construction updated ACSC website (Australian Signals Directorate, 2019d). However, the resources on these websites including a list of JCSC openings, monthly newsletters and information haven't been updated since mid-2018, making it difficult to find up to date information on the JCSC's initiatives and successes. Therefore, I have looked further for information.

The Centre for International Governance Innovation's 2018 report situates the JCSCs within the broader government structure, with a flow chart showing how the JCSCs will interact with other agencies (CIGI, 2018:15). However, it does not discuss the role of the JCSCs in relation to partnerships or relationships with the private sector, which is a major part of the JCSCs' goal, nor does it expand on the shift towards cyber security as a national security concern, but it does state the need for these discussions (CIGI, 2018).

The opening and impact of the JCSCs in each state has been reported in various media outlets, including newspapers such as the Courier Mail (Sigston, 2017), IT websites such as ComputerWorld (Pearce, 2017), and security industry magazines like the Australian Security Magazine (Admin, 2017) and Innovation Aus (McClure, 2018). The JCSC initiative is also mentioned in media releases from government departments such as the Department of Defence (2018) and public sector news sites such as The Mandarin (Easton, 2019).

1.2 Scope

The scope of this thesis is limited to publicly available Australian Federal Government policies related to defence, national security and cyber capability (both offensive and defensive) including Defence White Papers, Intelligence Reviews and Cyber Security Strategies. I have chosen to examine these documents for multiple reasons. First, these documents communicate the narrative that the government presents to the Australian public and the global community. Second, these documents are what guide the measures put in place and action taken by the government. In other words, these documents outline the strategic priorities of the Federal Government and outline what changes will be implemented across Australia's security landscape, including Australia's intelligence community, the Australian Defence Force and the Australian Federal Police to reflect these priorities. In addition, these documents provide a guideline of the government's priorities for private industry, highlighting key areas for expansion and research. This thesis does not discuss the process of creation and collaboration that result in these policies, rather it discusses the impact of these documents once they are made public.

Another reason this thesis is restricted to publicly available documents is because of the difficulty in getting access to classified and confidential documents. The 10-month time limit on this project made it difficult to access documents that are not publicly available. To further develop this project, I would seek to access information that is not publicly available. It is also important to note that this thesis does not seek to explain, or discuss, *why* discourses around cyber security have shifted as this would be beyond the scope of the 20,000 word limit of this thesis. However, this would be an area for further research, as will be discussed in Chapter 4.

1.3 Methodology

This thesis will engage with multiple methodologies to present a holistic picture of Australia's strategic priorities around cyber security, including discourse analysis, case studies, content and comparative analysis and interviews. This thesis also draws on the theoretical frameworks of Securitisation and Framing to discuss why the change in language in these policy documents is important and how it has influenced the practical measures put in place by the government and private industry.

1.3.1 Securitisation and Framing

While a relatively new approach in International Relations, constructivism has gained popularity (McDonald, 2008, Burgess, 2010). Constructivism differs from other approaches to security studies because it argues that reality is socially constructed, rather than relations between already existing states and identities (Mutimer, 2010). Constructivism is a broad field, but securitisation and the Copenhagen School has become one of the most influential approaches in international relations, and will be drawn upon in this thesis.

The Copenhagen School has been particularly influential in understandings of non-traditional security threats (McDonald, 2013). Securitisation is a term first used by Ole Wæver (1995) and explores the processes by which a topic, object or issue is turned into an existential threat through 'speech-acts', in order to justify addressing this security threat with harsher measures than would otherwise be acceptable (Wæver, 1995, Watson, 2012, McDonald, 2008 and Balzacq, 2010). McDonald (2013) argues that securitisation is most relevant to Western liberal democracies, as it relies on political debate and a communal consensus on the importance of an issue. It is therefore important to recognise that securitisation is not universally applicable, but rather functions in particular contexts to authorise the use of extraordinary measures to combat a perceived security threat (Wæver, 1995, Browning, 2017 and Burgess, 2010).

Securitisation has been employed in a variety of issues, and has become one of the most popular approaches to security, especially post 9/11 in reaction to U.S. involvement in Afghanistan and Iraq (McDonald, 2008), and the broader conditions that facilitate a

successful deployment in foreign conflict (Zimmermann, 2017). Securitisation has been employed to explore many contemporary issues, for example how Trump's administration worked to securitise Mexican immigrants (Browning, 2017). It has also been extremely influential in feminist branches of security studies, especially in the analysis of discourses about gender (Mutimer, 2010, Enloe, 1983 and Crow, 2017). Finally, securitisation has also been applied to energy security, particularly in the Middle East (Christou and Adamides, 2013).

The limitations of securitisation have also been well documented. One of the major critiques of securitisation and constructivism is the difficulty in measuring results (McDonald, 2013). It is difficult to prove when something has been securitised, and who the target audience of the securitisation process is (McDonald, 2013, Watson, 2009, Caballero-Anthony, Emmers and Acharya, 2006). Furthermore, securitisation theory does not allow for the existence of multiple audiences and their reception (Watson, 2009). In particular, *Non-Traditional Security in Asia* (Caballero-Anthony, Emmers and Acharya, 2006), challenges securitisation theory and provides case studies from the Asia-Pacific that expose and overcomes these weaknesses. Critiques of the securitisation of migration in particular include that securitisation does not account for variables that have their own norms such as racial violence (Moffette and Vadasaria, 2016). This means that other social and cultural factors influencing an issue can be overlooked unless the research engages with other theoretical frameworks and concepts (Moffette and Vadasaria, 2016).

Cyber security is a very broad and multidisciplinary field of enquiry, with discussions about cyber capability and power (Nikitakos and Mavropoulos, 2014), cyberspace from an international relations perspective (Fjäder, 2016) and cyber security policy (Loiseau and Lemay, 2012, Harknett and Stever, 2011). Securitisation and framing have been used to explore how policy and governments can address cyberspace by multiple authors. Dunn-Cavelty (2013) discusses the ways in which cyber threats are constructed through discursive practices, and the importance of this language. There is also a growing body of literature discussing the relationship between cyber security and national security and discussing the growing importance of both offensive and defensive cyber capability for different state actors. Kaplan (2016) focuses on the United States of America's state sponsored cyber capability, both offensive and defensive. Ventre's (2012) *Cyber Conflict: Competing National*

Perspectives examines the attitudes of different countries to cyberspace and the opportunities and challenges it provides for different states including Greece (Fitsanakis, 2012) and South Africa (van Niekerk and Maharaj, 2012). Nissenbaum (2005) adapts the framework of securitisation to compensate for the technical field of computer security, arguing that the shift from computer security to national security is due to a shift in language and intention in United States cyber policy.

1.3.2 Discourse Analysis

Discourse analysis has been applied to cyber security policy from a number of perspectives (Dunn-Cavelty, 2013). Barnard-Wills and Ashenden (2012) for example, use discourse analysis to critique the use of language in discussions about securing cyberspace. They argue that discourse is vital for constructing cyberspace as virtual space that needs to be governed by both social norms and state intervention (Barnard-Wills and Ashenden 2012). Discourse analysis also combines with Securitisation and Framing, as they are processes of threat creation and acceptance based on speech-acts (McDonald 2013). By examining and deconstructing the language used by the Australian Federal Government (or that any state), it is possible to see the impact that this language has had in shaping law enforcement responses and priorities. This methodology is adopted by Loiseau and Lemay (2012), together with historical analysis to write a history of Canada's security policy. This thesis draws on a similar body of literature, using discourse analysis combined with content analysis to examine how discourses around cyber security have changed over time. This method is complemented by the use of two case studies: the Joint Banking and Finance Sector Investigations Team and the Joint Cyber Security Centre initiative.

To further complement the discourse analysis, this thesis includes content analysis to provide quantitative analysis. Adding this data will provide quantitative evidence to further support the discourse analysis and demonstrate the dramatic shift in discourses over time. Furthermore, this mixed methodological approach helps to overcome the shortcomings and weaknesses of the individual methodologies.

1.3.3 Case Studies

While the discourse and content analysis outline the changes in language across major public documents like Defence White Papers, there are significant drawbacks to this method. The discourse analysis demonstrates how discourses around cyber security have changed, but it cannot show how these changes manifest in the creation of cyber security responses. Using case studies to support the arguments made in this thesis helps to bridge the gap between theory and its practical applications (Yin, 2009). The aim of this thesis is to not only analyse a change in discourse and language, but to demonstrate the practical implications and effects of these changes over time.

The JBFSIT and JCSCs have been chosen as the case studies for two reasons: first, they were both proposed under new initiatives to fight cybercrime. The JBFSIT was established under the Australian High-Tech Crime Centre, as announced in the 2000 Defence White Paper. The JCSC initiative was first proposed as part of the Australian Cyber Security Centre which was announced in the 2016 Defence White paper and 2016 Cyber Security Strategy. Second, they are both public/private initiatives designed to combat the predominant cyber threats to government and industry as flagged by the federal government documents. I have chosen to use these two case studies because they provide the opportunity to examine the ways in which the strategic directions outlined in Australian Federal Government documents impact Australia's security landscape. These case studies will provide evidence for the core arguments of the thesis, as well as demonstrate the relevance of the research by balancing the theoretical analysis and the practical implications. The similarities between the two case studies provide a set of parameters through which the similarities and differences between the two strategies can be compared, focusing on the points of difference the potential causes.

Case studies have significant advantages for the social sciences. Case studies are particularly well suited to research with a limited scope, as they provide the opportunity for research depth within a project with defined boundaries (Yin, 2009). For this thesis, using case studies allows for an in-depth analysis of two separate cases in order to provide further evidence for the central argument of this thesis. These case studies have been chosen for their common purpose, creation and influence on Australia's security landscape. A further advantage of using case studies is that they help to facilitate comparative analysis. By combining

information from a variety of sources in a way that moves beyond writing a historical account, to draw research conclusions about contemporary events and issues, particularly when they are still unfolding, such as with the JCSC initiative (Yin, 2009: 11). Case studies also combine well with other methodologies (Yin, 2009: 13). It is for these reasons that case studies are used in this thesis rather than historical analysis.

However, there are many critiques of the value of case studies. First, case study methodology has been critiqued for its lack of scientific rigour (Yin, 2009: 14). Case studies do not conform to traditional scientific measures of rigour and there is no standard for how case study methodology should be undertaken (Yin, 2009, Yin, 2012). This lack of established guidelines, combined with concerns of the empirical integrity of qualitative research methods such as participant-observation means that the case study method remains controversial in the social sciences (Yin, 2009, Yin, 2012). However, this can be minimised by engaging with multiple methodologies because it helps to negate bias by providing more and different types of data (Yin, 2009: 14). While case studies often include interviews and perspectives from participants in the events being analysed (Yin, 2009), due to a delay in ethics clearance, it was not possible for this thesis to contain interview data. However, this would be an area for further exploration as part of a larger project.

1.4 Conclusion

Cyber security as a national security issue is a growing field, with a growing body of literature in the key areas of critical infrastructure protection, public-private partnerships, information warfare and state-level cyber strategies. Within these discussions there is an overwhelming lack of literature discussing the evolution and trajectory of Australia's cyber security policies, and the impact of the language in these policies on Australia's security landscape. This thesis sits within this gap, examining the impact of changing discourses around cyber security in Australian Federal Government policy documents and the effect the changing discourses has on Australia's security landscape. The following section will use discourse analysis to argue that the language and terminology used to discuss cyber security has changed significantly since 2000, leading to cyber security being perceived as a national security issue.

2. The Evolution of Australia's Cyber Security Consciousness

This Chapter examines official Australian Federal Government policy documents including Defence White Papers, Independent Intelligence Reviews, National Security Strategies and Cyber Security Strategies to explore how discourses around cyber security have changed between 2000 and 2019. These documents have been chosen because they outline the strategic priorities of the Federal Government, and how these will be achieved. Also, these documents provide the narrative that the Government wants to convey to the public, thereby justifying actions that reinforce these priorities. This chapter will trace the change in discourse from that of a policing framework to that of a national security framework and show the way that the narrative around cybercrime has changed between 2000 and 2019.

This chapter will split Australia's Federal policies into three time periods: 2000-2009, then 2009-2013 and 2013-2019. I will argue that between 2000 and 2009, cybercrime was considered a policing matter, evident by the language used around cyber attacks and the minimal place they hold in the policies. From 2009 to 2016 however, there starts to be a shift in the language and considerations around cyber capability, with new initiatives and changes in government responses to cybercrime announced. Finally, between 2016 and 2019 we can see major changes in Australia's cyber policy and the structure of Australia's security landscape and intelligence community to reflect the increasing role of cyberspace for Australia. This thesis does not examine why this discursive shift has occurred, nor the processes through which the policies are created, rather it seeks to expose and this shift and its consequences for the Australian law enforcement and intelligence communities, which will be discussed in the following chapter.

2.1 The Rising Problem of E-Crime: 2000-2009

The first mention of cyber capability appears in the 1994 Defence White Paper, where cyber and information security is briefly discussed in section 5.81 (Department of Defence, 1994). This section discusses the different ways that physical and information security should be handled (Department of Defence, 1994:55). It states that information security is to be ensured in-house, rather than through third parties, as opposed to physical security which may be

undertaken by commercial security firms (Department of Defence, 1994: 55). The 1994 Defence White Paper also contains a more detailed section on Australia's key intelligence gathering agencies, identified as the Defence Intelligence Organisation and Defence Signals Directorate (now the Australian Signals Directorate), and leveraging technological advances to drive deeper knowledge of the strategic environment in order to protect Australia's secrets (Department of Defence, 1994). While this White Paper emphasises the importance of Australia's intelligence community, there is no provision for an expansion of information technology security, cyber incident management.

This is not surprising, given that the Federal Government had been resistant to incorporate the Australian Computer Emergency Response Team (AusCERT) into any government portfolio (Smith and Ingram, 2017). AusCERT was created in 1993 as a collaboration between the Queensland University of Technology, Queensland University and Griffith University in response to cyber attacks on government systems in the United States that were traced back to these universities (Smith and Ingram, 2017). As a result of the lack of government funding, AusCERT became a subscription-based service run by these universities and was Australia's key cyber security response until 2009, despite the lack of acknowledgement in any Defence White Paper or policy (Smith and Ingram, 2017). However, in 2003, sponsored by the Federal Government, AusCERT became responsible for national alerts on cyber incidents as part of the E-Security Initiative (Smith and Ingram, 2017: 650). Between 2003 and 2009 AusCERT was both unofficially and contractually utilised by the federal government to drive industry/government partnerships, receive cyber incident reports and disseminate information to business (Smith and Ingram, 2017: 650).

The 2000 Defence White Paper discusses cybercrime within the larger framework of the Australian Defence Force and the ways in which cyber attacks could impact Australia's National Information Infrastructure (NII) (Department of Defence, 2000). With developments and investments in technologies to facilitate and improve Australia's intelligence gathering capabilities, concerns related to cyber security focus on the protection of these assets (Department of Defence, 2000). The 2000 Defence White Paper discusses information warfare within a framework of information capabilities, including intelligence, information operations, logistics and business applications, surveillance capabilities and communications (Department of Defence, 2000: 94-95).

In the 2000 Defence White Paper, cyber attacks are specifically designated non-military threats, along with terrorism and organised crime (Department of Defence, 2000: 12). This places the responsibility for protecting against cyber attacks and cyber incidents as the responsibility of the civilian sector, with assistance from the Government provided in the case of critical infrastructure protection (Department of Defence, 2000). However, the White Paper specifies that this government collaboration would be in an advisory role and should not detract or distract from the key priority of protecting from armed attacks, and therefore civilian expertise would be predominantly applied to cyber responses (Department of Defence, 2000: 13).

It is interesting to note that 2000 Defence White Paper flags cyber attacks as a rising threat, and states that, "this new security challenge is being taken seriously by the Government, and a comprehensive national approach is currently being developed." (Department of Defence, 2000: 13). As a result, the 2001 E-Security National Agenda was published. The 2001 E-Security National Agenda further recognised the need for adequate measures to protect Australia's information infrastructure. It proposed that $2 million be allocated to assisting the DSD (now ASD), AFP, ASIO and the Attorney-General's Department identify and create policies and procedures to manage the emerging threats long term (Williams, 2001). Australia's E-Security National Agenda's intent was "to create a secure and trusted electronic operating environment" (MacGibbon 2009: 4) (Smith and Ingram, 2017: 652). However, Smith and Ingram (2017) argue that without proper government oversight, this led to a number of smaller groups and projects with no cooperation or communication between them (Smith and Ingram, 2017: 652).

In 2004, the Minster for Justice and Customs discusses the allocation of the responsibility for the E-Security National Agenda to the Australian High Tech Crime Centre and the Australian Federal Police's Computer Forensics division to capitalise on the opportunities for collaboration between the two (Commonwealth of Australia, 2004). This also created the base for the JBFSIT by establishing a task force solely dedicated to cybercrime.

Updates to the 2000 Defence White Paper were released in 2003, 2005 and 2007 in response to security incidents such as the 9/11 terrorist attacks and the Bali Bombings (Parliament of Australia, 2019). The 2003 Update focused on managing the threat of terrorism, particularly in relation to weapons of mass destruction (Parliament of Australia, 2019). The 2005 Update maintained the focus on terrorism and weapons of mass destruction, but also added the consideration of global and state stability and updated policies addressing the efforts of the Defence Force in the Middle East (Parliament of Australia, 2019). Finally, the 2007 Update further expanded upon priorities around regional stability and changes across the Asia-Pacific (Parliament of Australia, 2019).

2.2 Shifting Priorities, National Security and Changing the Security Landscape 2009-2016

The next Defence White Paper was released 9 years after the 2000 Defence White Paper titled 'Defending Australia in the Asia Pacific Century: Force 2030' (Department of Defence, 2009). The Minister's Preface of this report presents cyber warfare as a new and evolving concern to defend against, as well as an opportunity to advance and secure Australia's strategic interests (Department of Defence, 2009). Discussions of cyber warfare are integrated throughout the White Paper, including in relation to the ADF and special forces operations. The paper proposes what the Australian Defence Force, intelligence community and security landscape will look like moving towards 2030 based on the strategic priorities outlined in the paper. These priorities build off the 2000 Defence White Paper, but differ significantly in relation to the importance of cyber capability. Despite cyber capability development being identified as a major priority looking forward, the key priority remains the ability to defend against conventional armed attacks (Department of Defence, 2009). Aligned with this, there is also discussion of the desire to project both military and political power to advance Australia's strategic interests (Department of Defence, 2009). The 2009 Defence White Paper is also the first White Paper to use the term 'cybersecurity' (Department of Defence, 2009).

In a section dedicated to cyber warfare the 2009 Defence White Paper assigns primary responsibility for cyber warfare and security capability to the DSD, which will draw on

cooperation with the Attorney-General's department, private industry, the Cyber Security Operations Centre, ADF, AFP and the rest of the intelligence community (Department of Defence, 2009: 83). Later in the document, the Defence Science and Technology Organisation is also assigned research about and implementation of cyber warfare and security (Department of Defence, 2009).

Cyber warfare is identified as a threat to critical infrastructure, and a priority for development to secure Australia's strategic interests into the future (Department of Defence, 2009). Where cyber attacks were mentioned in the 2000 Defence White Paper purely in relation to critical infrastructure (or National Intelligence Infrastructure as it was called then), the 2009 White Paper discusses cyber attacks in more depth and connects them to the idea of 'cyber security' (Department of Defence, 2009). The 2009 Defence White Paper discusses cyber attacks as part of Australia's defence against an actor who may target Australia using aggressive warfare tactics including a mix of conventional force, intelligence-based operations and cyber attacks on government, defence and civilian systems (Department of Defence, 2009: 55). In these discussions, the Australia government acknowledges the growing importance of cyberspace for the general public and the government.

It is in Section 9.8 that the first concrete link between cyber security and national security is made, with the creation of the Cyber Security Operations Centre (CSOC), an organisation comprised of members of the ADF, DSD and DTSO "purpose-designed to serve broader national security goals" (Department of Defence, 2009: 83). The CSOC would work towards national security goals by coordinating responses to cyber incidents in the private and public sectors, supported by staff agencies that worked on e-crime prevention including the Attorney General's Department, the AFP and leveraging agency expertise where relevant (Department of Defence, 2009: 83).

A major point of difference between the 2000 and 2009 Defence White Papers is in the organisation of intelligence and electronic capability. Where the 2000 Defence White Paper segregated intelligence capabilities from cyber and electronic capabilities, the 2009 Defence White Paper combines discussions of electronic warfare, cyber security, national security and intelligence capability (Department of Defence, 2009). This speaks to the rising impact of technology and its effects on the entire security landscape and the connection between the

intelligence community and cyber security in defending against malicious actors as well as advancing Australia's strategic interests.

Part of the 2009 Defence White Paper specified that Defence White Papers would be released at least once every five years, after the nine year gap between the 2000 and 2009 White Papers and the major changes it imparted (Department of Defence, 2013). The 2013 Defence White Paper built on the priorities of the 2009 White Paper, further emphasising the importance of cyber security and cyber warfare, with a more centralised approach to cyber security and the announcement of the creation of the Australian Cyber Security Centre (ACSC) and the Cyber Security Operations Centre (CSOC) (Department of Defence, 2013). The 2013 White Paper discusses the importance of cyber security and the role that cyber capability could play in national security throughout the document, including in discussions about alliances, critical infrastructure protection, information sharing and in relation to the intelligence community (Department of Defence, 2013). In addition, this White Paper announced the renaming of the Defence Signals Directorate to the Australian Signals Directorate and the Geospatial Organisation Agency renamed as the Australian Geospatial-Intelligence Organisation to represent the growing roles of the agencies within Australia's intelligence community (Department of Defence, 2013).

The Attorney-General's office released the first National Security Strategy for cyber security in 2009 (Smith and Ingram, 2017: 652). This "articulated a set of principles, priorities and capabilities to achieve them" (Smith and Ingram, 2017: 652), including the creation of a national CERT (CERT Australia) and a new Cyber Security Operations Centre under the DSD (Smith and Ingram, 2017: 652). This followed the US' 2003 example of creating a national CERT to partner with CERT/CC (Smith and Ingram, 2017: 653).

The 2011 Independent Review of the Intelligence Community Report discusses cyber security and cyber warfare within the context of global power and the priorities for the Australian intelligence community (Cornall and Black, 2011). It also discusses how the different agencies interact with cyberspace and advocates for international dialogue around rules for cyberspace and cyber warfare (Cornall and Black, 2011). The review discusses the changes in the Australian intelligence community since the 9/11 terrorist attacks in the United States, and the increased collaboration between Australia and its allies to improve information sharing

and security (Cornall and Black, 2011). Much of the attention has been on terrorism and helping to secure Australia's security within the Asia-Pacific (Cornall and Black, 2011). The 2011 Independent Review of the Intelligence Community outlines the role of cyber capability within the intelligence community and how technology has impacted on the intelligence community's goals (Cornall and Black, 2011). While the review mentions that other states including China and the United States believe that cyber capability is valuable in conflict (Cornall and Black, 2011), it does not relate this to Australia's strategic priorities as in the 2013 Defence White Paper.

The 2013 Defence White Paper further expands on the domestic priorities for cyber capability as discussed in the 2009 Defence White Paper, and it is the first document to identify state sponsored cyber attacks from other countries as an issue. It complements the 'National Security Strategy' of 2013 and the 'Australia in the Asian Century White Paper' of 2012. In the 2009 Defence White Paper cyber attacks were discussed in terms of any malicious actor, but particularly terrorists, where the 2013 White Paper specifically mentions China as a state actor with notable cyber capabilities that Australia would need to consider (Department of Defence, 2013). This is a major change from previous official policy documents. The 2013 Defence White Paper also emphasises the importance of increasing government investment in cyber capability, both offensive and defensive (Ball and Waters, 2013). However, Ball and Waters argue that while the 2013 White Paper acknowledges the need for enhanced cyber capability, it lacks a strategic plan for how this will be achieved, particularly in terms of recruiting people with the skills to make these goals a reality (Ball and Waters, 2013). This is a recurring absence across many of the policies from 2013 onwards.

Also released in 2013 was a second national security strategy titled 'Strong and Secure: A Strategy for Australia's National Security'. This strategy outlines three key priorities to be achieved within a five year period: strengthening regional engagement with the aim of security and prosperity for the entire region, the development of partnerships across government agencies, private industry, the Australian public and between governments to drive innovation, and the creation of comprehensive and integrated cyber policies and operations (Department of Prime Minister and Cabinet, 2013: iii). Furthermore, the strategy identifies including malicious cyber activity as one of the seven risks to national security (Department of Prime Minister and Cabinet, 2013, Brookes, 2015). Discussions of cyber security in this report address both cybercrimes that affect the general public like identity theft

as well as organised crime and state-sponsored cyber espionage (Department of Prime Minister and Cabinet, 2013).

Fundamentally this strategy advocates for greater communication and collaboration to combat cybercrime in all its forms (Department of Prime Minister and Cabinet, 2013). In terms of cyberspace, the strategy discusses streamlining processes and facilitating intelligence sharing across State Police and multi-agency taskforces (Department of Prime Minister and Cabinet, 2013). Discussions of national security threats emerging from cyberspace are much more comprehensive. The strategy identifies that traditional alliances such as those with the United Kingdom will need to be updated and re-evaluated to include cyber threats, as with the expansion of ANZUS to include cyber threats in 2011 (Department of Defence, 2016, Smith and Ingram, 2017). The 2013 National Security Strategy also further discusses the creation, purpose and resources of the Australian Cyber Security Centre (Department of Prime Minister and Cabinet, 2013).

2.3 A New Era in Cyber Security: 2016-2019

The 2016 Defence White Paper was released with the idea of being the most comprehensive plan to prepare for advancing Australia's strategic interests until 2035 (Department of Defence, 2016). It defines strategic priorities based on a changing and complex geopolitical environment and highlights the importance of both offensive and defensive cyber capability for both national and economic security (Department of Defence, 2016). It details plans to create 1200 jobs across space-based capabilities, intelligence and cyber security to further support the security sector (Department of Defence, 2016). This is complimented by an extra 900 cyber capability-based jobs in the Australia Defence Force, particularly to support special forces operations (Department of Defence, 2016).

The 2016 Defence White Paper frames discussions of cyberspace and cyber security as an essential part of Australia's national security, and cyber attacks as one of the greatest threats to Australia (Department of Defence, 2016). This threat is discussed both in relation to the Australian Defence Force, and the impact on private industry (Department of Defence, 2016). It also explicitly mentions the need for Australia to mitigate cyber threats from both state

actors and non-state actors (Department of Defence, 2016). Where the 2013 Defence White Paper referenced state-sponsored cyber attacks as an important threat to counter, the 2016 Defence White Paper refers to cyber attacks as "non-geographic" (Department of Defence, 2016:41).

Cyber attacks are also discussed as tools of conflict, with the 2016 Defence White Paper identifying that the conflict between the United States and China is not just about physical conflict and friction, but also friction in cyberspace (Department of Defence, 2016). The White Paper identifies that this friction has the potential to further escalate tensions between the two major powers (Department of Defence, 2016). In this way, cyber capability is discussed as an active part of the conflict between states, further emphasising the importance of cyber security. There is also a large section in the 2016 Defence White Paper discussing the importance of having space- based capabilities to ensure access to satellites and other systems of communication in space (Department of Defence, 2016). Space-based capabilities are mentioned briefly in the 2013 Defence White Paper, but were mentioned in collaboration with cyber capability. As with the 2013 Defence White Paper, intelligence and cyber capability are discussed together but with the addition of electronic warfare and surveillance and reconnaissance in the 2016 Defence White Paper.

2016 also saw the release of 'Australia's Cyber Security Strategy: Enabling Innovation, Growth and Prosperity' a report that outlines Australia's strategic direction related to cyber security, especially in relation to national security. In this report, the capabilities of Australian Cyber Security Centre are emphasised in terms of partnerships with industry, operation beyond its intelligence roles, and new capabilities for intelligence sharing (Australian Government, 2016, Smith and Ingram, 2017: 654). However, the ACSC and CERT Australia still operate under the ASD (Australian Government, 2016, Smith and Ingram, 2017: 654). Smith and Ingram express concern that the association with the militarised security and intelligence gathering of the ASD may hamper the trust and relationships that occur with CERT Australia and the ACSC, as most cyber activity occurs within the civilian sphere (Smith and Ingram, 2017: 654). They also highlight the ambiguity in language in discussing the relationships between government, agencies and private industry, with a focus on taking responsibility, but lacking clear language on how this will take place (Smith and Ingram, 2017: 654-5).

In 2017, the Federal Government released an update in progress for the Cyber Security Strategy of 2016, outlining successes and areas to work on (Australian Government, 2017). This included a table showing which agencies and departments are responsible for the different cyber security goals, with most assigned to the Attorney-General's Department, Department of PM and Cabinet, Department of Defence (Australian Government, 2017: 25-29). Both the 2016 strategy and the 2017 review emphasise the importance of cyber security and cyber warfare to Australia's national security, with little mention of the traditional cybercrime of the 1994 and 2000 Defence White Papers. Also, there is no mention of the AFP or agencies and divisions like the AHTCC, further proving that there has been a shift away from cybercrime as a policing concern to that of national security and defence.

The 2017 Independent Intelligence Review discusses a shift in the distribution of Australia's cyber security and capability (Department of Prime Minister and Cabinet, 2017). This review highlights the need for greater information sharing and cooperation across the Australian intelligence community, facilitated by the creation of the Office of National Intelligence (ONI) (Department of Prime Minister and Cabinet, 2017). These priorities are reflected in the designation of the ACSC and cyber security to the ASD, under the Minister for Defence (Department of Prime Minister and Cabinet, 2017). The emphasis in this review is on streamlining the power structure of the intelligence community to achieve the best results, including a hierarchical chain of command for cyber security (Department of Prime Minister and Cabinet, 2017).

2.4 Mapping the Changes

Across the Defence White Papers there is a shift away from policies and direction related to purely conventional warfare, and towards the consideration of non-traditional threats and the rising importance of leveraging cyber warfare and cyber security. It is also clear from the 2013 White Paper onwards that the threat of cyber-attacks come from both state and non-state actors, and impact both government and private industry in ways that the earlier White Papers had not considered. This speaks both to advances in technology as well as the rising importance of preparing for non-traditional threats in addition to conventional warfare. It is

also important to note the development of policies that integrate the Australian Intelligence Community into discussions around cyber capability.

This is further supported by the Independent Intelligence Reviews, both of which contain a discussion of cyberspace as a key influencer in the way Australia interacts with the rest of the world, particularly in geopolitics and cyber warfare. This demonstrates the ways in which the Australian intelligence community perceive the impact and importance of cyber security and cyber capability or Australia. There is a greater focus on the impact of cyberspace on Australia's security priorities in the Independent Intelligence Reviews than in the Defence White Papers.

The National Security Strategies outline the strategic priorities of the Federal Government across the 19 years, further showing a shift away from traditional threats and military action and towards combatting and managing non-traditional security threats. In the policies closer to the 9/11 terrorist attacks in the United States, much of the policy is centred around combatting terrorism in collaboration with Australia's allies, including the United States and the United Kingdom. The 2013 Defence White Paper and 2013 National Security Strategy set the scene for increased international cooperation in order to combat threats and cyber attacks from both non-state actors and state sponsored actors.

Across all of these policies, there is a clear shift in the way the Federal Government talks about cyber security and its role in Australia's security landscape. Between 2000 and 2009, cyber security is predominantly discussed through terms like 'technology-enabled crime' and 'National Information Infrastructure', with law enforcement responses created within law enforcement bodies like the Australian Federal Police. Between 2009 and 2016 the shift in language begins, with the release of policies like the 2009 Defence White Paper and the National Security Strategy for cyber security, which start to discuss the role of cyber security and capability in Australia's threat landscape. These documents still see cyber security as less of a concern than traditional threats and the threat of terrorism, but there is an awareness of the importance of cyber space for Australia's economy and security. In order to address this, new initiatives such as the Australian Cyber Security Centre are created under the Defence Portfolio and the Attorney-General's Department. The 2016 Defence White Paper and the 2016 Cyber Security Strategy emphasise the importance of cyber capability for Australia and

discuss the risks of cyber warfare and the importance of Australia having a comprehensive cyber security strategy. In comparing these policies to those of from 2000-2013, the shift in discourse is obvious, with terms like ‘information warfare’, ‘cyber security’ and ‘critical infrastructure’ replacing the earlier terminology.

2.5 Conclusion

This chapter has shown the development of Australia’s cyber security awareness, and how discourses around cyber have changed from that of a policing and cybercrime framework to one of national security. The language used in these policies has real world impacts on the way that Government cyber responses are structured. The next section will demonstrate the impact of the militarization and securitisation of cyber security using two case studies, the JBFSIT and the JCSC.

3. Case Studies

This chapter builds on the analysis from the previous chapter, and will demonstrate the effect of the shift in discourses on Australia's security landscape using two case studies, the Joint Banking and Finance Sector Investigations Team and the Joint Cyber Security Centre initiative. Each organisation will be discussed in terms of the cyber environment at the time to show the impetus for creation of the case studies. Then I will discuss the creation and oversight of each case study, the strategic goals and how they were achieved, and the impact of each case study.

Fundamentally, these two case studies have the a very similar purpose, process of formation and strategic goals. The final chapter of this section will contain a comparative analysis of the key points of the case studies. This will show that the difference in these case studies really comes down to how they reflect the strategic priorities of the Federal government of the time as expressed through the language and narrative of Australia's cyber security policies.

3.1 The Joint Banking and Finance Sector Investigations Team

The early 2000s saw a rise in a new type of fraud, leveraging systems of internet banking and taking advantage of human weakness to convince consumers to provide their personal information and passwords. In response to this, the Joint Banking and Finance Sector Investigations Team (JBFSIT) was created under the Australian High Tech Crime Centre in 2004. This chapter will examine the JBFSIT by first exploring the cybercrime landscape between 2003 and 2004, then it will discuss the creation and formation of the AHTCC and how it relates to the JBFSIT. Finally, this chapter will unpack the JBFSIT. Together, this chapter will demonstrate how law enforcement responses to cybercrime are influenced by the strategic priorities as set out by the Federal Government policies discussed in Chapter 2.

3.1.1 A New Type of Crime: Phishing and the Banking Sector

2003 saw a dramatic rise in the prevalence of phishing scams across many areas of e-commerce (Rusch, 2005). The banking sector in particular was heavily impacted, with banks across Australia, the United States and the United Kingdom left scrambling to manage the rise in fraud resulting from phishing scams (Finextra, 2004, Rusch, 2005). To manage phishing scams, the banking sector tried to implement anti-phishing strategies and new measures for identity verification including the use of tokens, multi-factor verification and pushing for more education around phishing emails (Young, 2004). The United Kingdom in particular struggled to find cost-effective anti-phishing strategies (Young, 2004). In 2004 the number of phishing scams increased up to 10 times the number from the previous year with more than 18 million phishing emails being intercepted by MessageLabs, a UK based security software provider (Finextra, 2004). In Australia alone, it is estimated that banking fraud rose to $25 million in 2004 (Cincotta, 2007), and £4.5 million in the United Kingdom (Leyden, 2004).

The first phishing attack on an Australian bank occurred in March 2003, and was the first major phishing attack globally (McCombie, 2008, McCombie and Pieprzyk, 2010). Australian Banks targeted by these attacks include the Commonwealth Bank of Australia (CBA) in March 2003, ANZ in April 2003 and Westpac in June 2003 (McCombie, 2008). By June 2003, Australian banks had become aware of the phishing scams, and so Westpac were able to report the scam much faster than the CBA or ANZ to the Australian Federal Police, who had been involved in the investigations of the previous attacks (McCombie, 2008). These attacks were traced to websites hosted by companies in the United States and Ukraine, leading the AFP to contact the internet service providers to have the scam sites shut down (McCombie, 2008, McCombie and Pieprzyk, 2010). At this time similar attacks occurred targeting the Bank of America, Citibank and the First Union Bank, which were investigated by the Federal Bureau of Investigation (McCombie, 2008).

Globally, phishing incidents rose from 21 emails in November 2003 to 136 in January 2004 as recorded by the Anti-Phishing Working Group (McCombie and Pieprzyk, 2010). For Australian internet users, Phishing emails rose to 13,141 by January 2005, from 107 in December 2003 (Krone, 2005). These statistics demonstrate how quickly phishing scams escalated to become a major concern for e-commerce and the banking sector. Numbers

concerning phishing emails have continued to rise, with phishing remaining one of the top concerns for the banking sector (Accenture, 201). Therefore, it is an ongoing battle between phishing scammers and banks to become more tech savvy and find new ways to manage this crime (McCombie and Pieprzyk, 2010). Phishing first came to the attention of the Australia Hi-Tech Crime Centre in early 2003 (Bajkowski, 2004b). This prompted the AHTCC to work to foster relationships with the banking sector to discover how best to tackle the rising cost and risk of banking fraud from phishing scams (Bajkowski, 2004b).

3.1.2 The Australian High Tech Crime Centre

The Australian High Tech Crime Centre (AHTCC) was created in 2003 to combat the rise in prevalence of cybercrime, and began with 13 staff and a budget of $4 million (Platypus, 2009, SMH, 2003). The AHTCC was designed as a collaboration between the Australian federal government and private industry to combat and manage the rising threat of 'technology enabled crime', and to create a national platform to coordinate responses to technology enabled crime (AHTCC, 2008a, Platypus, 2009). Furthermore, the AHTCC was responsible for protecting Australia's National Information Infrastructure, and assessing the financial impact of technology enabled crime, of which the banking sector was a key part (Bajkowski, 2004b). One of the first tests of this capability came with the rise of phishing scams targeting e-commerce and the banking sector. The AHTCC needed to become involved in dealing with the new issues around phishing scams (Bajkowski, 2004b).

The AHTCC was a collaborative effort, with a large number of staff from the Australian Federal Police, complimented by police from each state and territory (Australian Federal Police, 2004). In addition to this, the AHTCC seconded staff from the Defence Signals Directorate, Australian Bureau of Statistics and the Australian Institute of Criminology among others (Australian Federal Police, 2004, Platypus, 2009). To more effectively address the transnational nature of what was termed 'high-tech crime', the AHTCC also utilised the Australian Federal Police's International Network to further develop relationships with agencies from the United Kingdom, the United States, Canada, Germany, Interpol and the G8 (Australian Federal Police, 2004: 41). These relationships included operations, intelligence sharing and training exercises (Australian Federal Police, 2004: 41).

Furthermore, the AHTCC engaged with private industry in one of the world's first ongoing public-private partnerships (Platypus, 2009). The AHTCC solicited assistance from the big 5 banks, the telecommunications sector and software providers like Microsoft (Platypus, 2009). The AHTCC also had a number of allied organisations including The Office of Film and Literature Classification (OFLC), The Attorney General's Department (AGD), NetAlert, the ABC and AusCert (AHTCC, 2004c). Most of these agencies and departments work to provide information about internet safety to the general public with some agencies like NetAlert focusing on educating children about the dangers of the internet (AHTCC, 2004c). The AHTCC's role was to provide information to the public on cybercrime prevention and mitigation as well as to provide a platform to report cybercrime (Platypus, 2009, AHTCC, 2004a). This information was made available through media releases on the AHTCC website (AHTCC, 2004a).

The AHTCC was an information and intelligence initiative, with no operational law enforcement capability (AHTCC, 2004b). They acted as a site for cooperation, intelligence gathering, monitoring and coordination (AHTCC, 2004b). This created a central location for information for both law enforcement and private industry, facilitating information exchange between different and competing companies, which the AFP could then act on in cooperation with state police (Platypus, 2009). Having this central information hub helped to facilitate coordination between law enforcement agencies to find and prosecute scammers all across Australia (Platypus, 2009). The AHTCC also had strong collaborative ties with the Australian intelligence community, partnering with the Defence Signals Directorate (DSD, now ASD) and Australian Security Intelligence Organisation (ASIO) to provide information on threats to critical infrastructure (AHTCC, 2004b).

3.1.3 The Joint Banking and Finance Sector Investigations Team

The Joint Banking and Finance Sector Investigations Team was created as a part of the AHTCC (Platypus, 2009, Australian Federal Police, 2004). It combined government resources from the Australian Federal Police (AFP), state police, and the banking sector to share information to prevent consumers falling victim to these scams as well as damage mitigation (Platypus, 2009). The JBFSIT was unique because it was one of the first public-private partnerships to second staff from other organisations (Platypus, 2009). It was designed to provide new insight into combatting hi-tech crime, particularly the rise of phishing scams in

the banking sector by combining the industry specific knowledge of the banking sector with the expertise of the Australian Federal Police and the Australian High-Tech Crime Centre (AHTCC) (Australian Federal Police, 2004). It also encouraged the law enforcement staff to focus more on education, mitigation and prevention and less on traditional policing methods (Platypus, 2009: 7).

The JBFSIT consisted of AHTCC staff and seconded staff from the Commonwealth Bank, ANZ, Westpac, St. George and the National Australia Bank (Bajkowski, 2004a, Australian Federal Police, 2004). The JBFSIT also had the support of VISA International, MasterCard, the Credit Union Society Corporation of Australia and the Australian Bankers Association (Bajkowski, 2004a, Australian Federal Police, 2004: 41). This meant that the JBFSIT could capitalise on the expertise and knowledge held by each organisation and provide an Australia-wide response to the rise of phishing scams (McKenzie, 2006). The JBFSIT began with staff from the AHTCC and the AFP along with five full time staff seconded and paid for by the banks listed above, or the major five banks (Bajkowski, 2004a, Bajkowski, 2004c, McKenzie, 2006). The JBFSIT was one of the first of its kind in the world, combining industry and government in a public-private partnership (Platypus, 2009). The JBFSIT also worked closely with AusCERT for incident response and technical support (McKenzie, 2006, Department of Defence, 2013).

McKenzie (2006: 34) identified that in 2006, the JBFSIT still maintained the five full time staff seconded from the banking sector, along with 17 AFP staff, one staff member from Queensland, Northern Territory, Western Australia, South Australia, Tasmania and Customs as well two staff members from the Victoria and New South Wales Police. All wages were paid for by their respective employers and funding sourced from the AHTCC budget (McKenzie, 2006). By the 31st of October 2006, the JBFSIT was comprised of six staff seconded to the AHTCC from the AFP, NAB, CBA, and the Northern Territory Police Service (Parliament of Australia, 2006b). For that year, the JBFSIT had resulted in three arrests with court cases ongoing and more referrals made to State and Territory Police (Parliament of Australia 2006b).

In August 2008 a second office of the JBFSIT was opened in Melbourne, to further enhance communications between the AFP and the banking sector (AHTCC, 2008b). Interestingly,

there is no mention of collaboration with the State and Territory Police, who had been a major part of the JBFSIT when it first opened in 2004. As of late 2008, the JBFSIT consisted of staff from the AFP, five seconded staff from the banking sector and technical specialists, and was housed within the AFP offices in Sydney and Melbourne (Australian Federal Police, 2009). This is a change from the original blueprint of the JBFSIT with the removal of the staff from each state and territory police. Furthermore, the original scope of the JBFSIT expanded from predominantly phishing scams to all online fraud (Australian Federal Police, 2009).

3.1.4 Strategic Frameworks of the AHTCC and the JBFSIT

The role of the AHTCC was threefold; first, the AHTCC provided "a national coordinated approach to combating serious, complex and multi-jurisdictional technology enabled crimes, especially those beyond the capability of single jurisdictions" (AHTCC, 2006). Second, the AHTCC assisted in improving the ability to manage 'technology enabled crime' across all jurisdictions (AHTCC, 2006). Finally, the AHTCC supported the protection of the National Information Infrastructure (AHTCC, 2006).

To do this, the AHTCC identified five main functions; co-ordination, investigation, liaison, intelligence and knowledge (AHTCC, 2006). While these functions are different, they overlap to create a holistic approach to high tech crime management. Coordination between state, federal and international law enforcement agencies overlaps with liaison with government, industry and international parties on technical, business, policy and investigative matters related to technology enabled crime to show the connections between business and law enforcement (AHTCC, 2006). Intelligence services leading to more understanding of the crime environment, particular in relation to technology related crime and investigations run by the AHTCC or referred to partner agencies together provide the overview of the crime landscape and how the threat of high tech crime can be handled (AHTCC, 2006). All of these functions help to provide knowledge of issues surrounding high tech crime and lead to measures to address it including education and training, best practice for investigations and tools, preventative measures and expert advice (AHTCC, 2006).

The JBFSIT had three main goals; first, to identify the people involved in phishing scams and malicious software to perpetrate financial fraud (2006). Second, the JBFSIT worked to foster

collaboration and information sharing with the private and public sectors including the major Australian Banks, the Australian Federal Police and State and Territory Police to figure out how best to manage the rising rate of financial fraud, especially through phishing. The JBFSIT's third goal was to minimise, mitigate the impacts of and provide evidence to lead to successful prosecution of financial fraud (AHTCC, 2006, McKenzie, 2006).

To achieve these priorities, the JBFSIT would conduct investigations using information from both the law enforcement and the banking sector (McKenzie, 2006, Bajkowski, 2004b). This information would be used to create an operational brief that would be used to guide law enforcement operations (McKenzie, 2006, Parliament of Australia, 2006a). As part of these investigations, the JBFSIT would trace the transactions and locations of money transferred through Australian money mules and large companies like MoneyGram and Western Union (McCombie, 2011). By identifying the Australian money mule, or the person helping to facilitate the transfer of money out of the country, the JBFSIT team could the trace where the money was being sent to, and liaise with the companies transferring the money to block the transactions (McCombie, 2011). This allowed the JBFSIT to shut down mule recruitment sites, malware download sites (Parliament of Australia, 2010).

In 2006 the senate recommended that the AHTCC and Australian Crime Commission (ACC) look into creating a subscription based service to provide information on fraud trends to industry, as the AHTCC and ACC were already working together to address financial crimes against the banking sector (Parliament of Australia, 2006a). This became part of the JBFSIT's role, to provide 'intelligence and operations assessments' providing current information on the threats, vulnerabilities and trends to the banking and finance sector (Parliament of Australia, 2006a). This helped to provide new knowledge and continue to update industry and government partners about the evolving crime landscape, including best practice, strategies to minimise the threat of financial fraud and share intelligence on emerging and current threats.

Within the framework of the AHTCC, the JBFSIT provided a coordinated approach to investigations with the banking sector, AFP and State Police, as well as liaising with AusCERT and seconding staff from the Australian intelligence community when required (Parliament of Australia, 2006a). This allowed for more comprehensive investigations into financial fraud, especially through phishing, and the collection of intelligence across the banking sector. With these measures, the JBFSIT could then liaise with international partners,

government agencies and private industry across technical, policy, business and investigative matters to help the AHTCC provide the nationally coordinated approach to technology enabled crime.

3.1.5 Strengths and Weaknesses of the JBFSIT

Alastair MacGibbon, Director of the AHTCC at the time of the formation of the JBFSIT, identified the building of relationships between the AHTCC and the banking sector, particularly of the big 5 banks, as being one of the main strengths of the JBFSIT (Bajkowski, 2004b). The JBFSIT was about cooperation between government and private industry in a public-private partnership (Australian Federal Police, 2004). Much of the rhetoric around national information infrastructure invoked this idea of the public-private partnership (PPP) to solve complex problems facing both industry and the government (McKenzie, 2006, Bajkowski, 2004b). MacGibbon said that the JBFSIT was a test to see whether industry and government could work together to produce better outputs than other methods (Bajkowski, 2004b).

One of the advantages of the JBFSIT was that it allowed for different skill sets to be combined (Bajkowski, 2004c). By seconding staff from both the banking sector and the AHTCC, the JBFSIT gained the benefits of both the banking sector's knowledge of how to best gather information and move through the sector, and the AHTCC staffs' advice and skills in advising what changes should be made (Bajkowski, 2004c). However, as a public-private partnership (PPP), the JBFSIT had to balance the interests of private industry, in this case the banking sector, with the interests of the Federal Government and law enforcement. MacGibbon identifies this as the biggest challenges he found as director of the AHTCC (Bajkowski, 2004b). In order to create a cohesive taskforce with common goals, MacGibbon and the AHTCC staff had to gain an understanding of the banking sector and how they respond to both cyber and physical incidents, and examine how the responses to the two differed (Bajkowski, 2004b).

With any PPP there are chances for the parties involved to take advantage of access to information and capability beyond what their individual organisation possesses, which can lead to abuses of information (McKenzie, 2006 and Bajkowski, 2004c, Carr, 2016). In the

case of the JBFSIT, MacGibbon identified that the AHTCC could have taken advantage of the connection to the banking sector and access information (Bajkowski, 2004c). For the banking sector, they could have hidden or worked together to hide pertinent information and misdirect the AHTCC staff (Bajkowski, 2004c). However, the use of strict non-disclosure agreements from all parties in the JBFSIT, clear boundaries and shared operational goals, as well as the benefit of the taskforce for all parties and government oversight and reports to the Senate, as well as the oversight from the AFP minimised this risk.

One of the strengths of both the JBFSIT and the JCSC was the incentive and encouragement they provide private industry to report cyber incidents (McKenzie, 2006, Bajkowski, 2004c). Participants in McKenzie's research expressed that while the banking sector had agreed to provide information about cyber incidents to the AFP, it wasn't until the JBFSIT that accurate, timely and comprehensive reports were provided (McKenzie, 2006: 310). The banks were disincentivised from reporting cyber incidents because of a fear of loss of consumer confidence if the knowledge were to become public (McKenzie, 2006). AFP and AHTCC staff in the JBFSIT were also provided with knowledge from the banking sector they would not have otherwise been able to access (McKenzie, 2006, Bajkowski**,** 2004c). As with the banking staff, the AFP and AHTCC staff signed confidentiality agreements, thereby guaranteeing the secrecy of the banks' information and taking away the perceived incentive to avoid reporting cyber incidents (McKenzie, 2006).

Furthermore, the JBFSIT encouraged collaboration from usually competing companies in a bid to combat a threat that threatens the entire industry (McKenzie, 2006). By uniting the banks to combat the challenges facing the entire industry, particularly the risk of consumers losing confidence in online banking, the JBFSIT could work collaboratively and pool resources to better address financial fraud (McKenzie, 2006). With all staff signing confidentiality agreements and the segregation of information to only allow access to the information each party needed to know, the banking sector could trust that their information wasn't going to be abused by any of the collaborating partners of the JBFSIT (McKenzie, 2006). This removed a major barrier to industry-wide collaboration and is one of the reasons the JBFSIT was so successful (Bajkowski, 2004c, McKenzie, 2006).

One of the criticisms of the JBFSIT, at least initially was the lack of notable prosecutions (Bajkowski, 2004b). This concern was shared across all operations addressing high tech

crime, especially financial fraud and phishing scams. The 2001 Cybercrime Legislation presented the first avenue for law enforcement to prosecute cybercrime in Australia however it hadn't been widely used to prosecute technology enabled crime (Bajkowski, 2004b). With the JBFSIT operational in 2004, law enforcement were testing how to investigate, prosecute and provide evidence for cybercrime to result in successful prosecutions (Bajkowski, 2004b, Bajkowski, 2004c). According to MacGibbon, the JBFSIT was the first time the amendments to the 2001 Cybercrime Legislation had been used, which led to a trial and error-based approach with the AHTCC learning what types of evidence and information would be needed for successful prosecutions (Bajkowski, 2004b).

There were also arguments that the banking sector didn't do enough to address the problem of phishing scams before they became a major financial cost to the banks (Gray, 2004). The banking sector acknowledged the importance of education to help consumers, but didn't believe it was their responsibility, rather the role of the Federal Government (Gray, 2004). This education later became part of the AHTCC's collaboration with AusCERT, the banking sector, and the AFP for both the banking sector and consumers (Parliament of Australia, 2006).

3.1.6 Integrating Capability and the AFP

In 2008, the AHTCC became part of the AFP's High-Tech Crime Operations (Platypus, 2009). This merger combined the research, prevention and industry cooperation with the operational capabilities of the AFP and expanded the purview of the AHTCC to other areas of cybercrime including child exploitation, terrorism and organised crime (Platypus, 2009). The merger also meant that all cybercrime responses became part of a single department, and integrated the information gathering capability with the operational capability (Platypus, 2009). However, this merger also handed control to the AFP and minimised and excluded state police from this network.

3.1.7 Lasting Impact

The JBFSIT was one of the first public-private partnerships between a Federal Government and the banking sector in the world (Platypus, 2009, Bajkowski, 2004c, McKenzie, 2006). The JBFSIT removed barriers and facilitated information sharing and cooperation across the sector and with law enforcement to combat the rise in financial fraud and phishing scams. As such it created the benchmark for PPPs both in Australia and around the world. While the JBFSIT was not without its challenges, fundamentally it proved that combining the expertise of the private sector and the public sector helps to provide insight that otherwise would not be possible.

3.2 Joint Cyber Security Centre Initiative

Between 2009 and 2016, major changes occurred across Australia's security landscape, with a noticeable increase in cyber attacks targeting government systems. This combined with a rise in everyday usage of the internet and increasing reliance on the digital economy led to the creation of new government funded bodies such as CERT Australia and the Digital Transformation Agency. This chapter will examine the Joint Cyber Security Centre (JCSC) initiative by first discussing cybercrime and political landscape and the major changes that led to the revision of government policy. Then, I will discuss the creation and formation of the Australian Cyber Security Centre (ACSC), and its connection to the JCSC. Finally, this chapter will examine the history, impact and role of the JCSC and demonstrate how the Federal Government's attitudes towards cyber security have changed. Furthermore, I will discuss how this affected national security discourses and government initiatives like the JCSC.

3.2.1 Setting the Crime Scene: The National Security Dilemma

As discussed in Chapter 2, the Attorney-General's Department released the Australia's first Cyber Security Strategy in 2009, aimed at coping with the rise of malicious activity that accompanied increased internet use by both businesses and individuals (Attorney-General's Department, 2009). The 2009 Cyber Security Strategy sets the scene for the priorities of the Federal Government that are further elaborated in the 2016 Cyber Security Strategy. The priorities of the 2009 Cyber Security Strategy include education programs to inform the public and business about cyber safety, developing a cyber-skilled workforce, partnering with other organisations to help develop research and solutions to cyber threats and the protection of ICT systems (Attorney-General's Department, 2009).

In order to achieve these goals, the 2009 Cyber Security Strategy announced the creation of two new government-sponsored bodies; CERT Australia and a new Cyber Security Operations Centre (Attorney-General's Department, 2009). CERT Australia was created under the Attorney-General's Department in 2010 in order to provide a point of contact for businesses and individuals affected by cyber incidents (Attorney-General's Department, 2009, Slocombe, 2013). The CSOC was created within the DSD (now ASD) with expert staff to

conduct operations and threat analysis in collaboration with Australia's intelligence community and international partners (Attorney-General's Department, 2009, Department of Defence, 2013, Slocombe, 2013). Between 2011 and 2012, the Cyber Security Operations Centre recorded more than 400 significant cyber incidents targeting government systems (Department of the Prime Minister and Cabinet, 2013). Furthermore, in 2012 the cost of cybercrime to Australia's economy reached $1.65 billion (Department of the Prime Minister and Cabinet, 2013). These figures show the importance of the internet for Australia's economy.

In 2013, Luiijf, de Graaf and Besseling (2013) analysed the National Cyber Security Strategies of 19 countries both large and small, including the Five Eyes. From this study, they identified that while critical infrastructure (CI) protection was flagged as an issue across all 19 countries of the study, Australia and Canada were the only two countries to specify a connection between CI protection and national security in their National Cyber Security Strategies (Luiijf, de Graaf and Besseling, 2013). Nonetheless, while Australia's 2009 Cyber Security Strategy made the connection between CI protection and national security, many scholars have argued that this policy failed to translate into practice, leaving Australia behind countries like the UK, the US and China (Smith and Ingram, 2017, Austin and Slay, 2016a, Austin, 2016, Austin and Slay 2016b).

As argued in Chapter 2, the 2013 Defence White Paper was the first policy document to discuss cyber security as being linked to national security and cyberspace (Department of Defence, 2013). It implemented changes to reflect these priorities including changing the Defence Signals Directorate to the Australian Signals Directorate (ASD) to reflect the growing role and cross-agency collaboration between the ASD and other intelligence agencies (Department of Defence, 2013, Jennings and Feakin, 2013). The 2013 Defence White Paper also expanded on the role of the ACSC and its close ties to Defence and the ASD (Department of Defence, 2013, Jennings and Feakin, 2013).

Across 2013, the DSD responded to 940 cyber incidents targeting government systems, 37% more than 2012 (Department of the Prime Minister and Cabinet, 2014). With such a rise in cyber incidents and with 73% of Australians using the internet at least once a day, finding ways to secure cyberspace became increasingly important (Department of the Prime Minister and Cabinet, 2013). These statistics also show the rising threat to government systems and

critical infrastructure. The Defence Science and Technology Organisation's (DSTO) report (2014) argues that Australia's increasing dependence on the internet across the general population, essential services, critical infrastructure and in Government has led to a range of new threats and vulnerabilities that must be managed and addressed. This was demonstrated in the #Censusfail incident, a Distributed Denial of Service attack on the Australian electronic census in 2016 (Office of the Cyber Security Special Advisor, 2016).

On 13 October 2016 the Office of the Cyber Security Special Advisor released a report investigating a cyber incident that took place on the Census night in 2016 (Office of the Cyber Security Special Advisor, 2016). This report exposed the flaws in communication, preparation and investment that could have prevented or minimised the DDoS attack (Office of the Cyber Security Special Advisor, 2016). It also criticises and critiques the decisions made by all parties leading up to the incident including a lack of clarity around roles and responsibilities of IBM and the ABS, and provides a set of recommendations to prevent a similar incident occurring again (Office of the Cyber Security Special Advisor, 2016). This incident and the response from the Office of the Cyber Security Special Advisor demonstrates the new types of threats and vulnerabilities expressed in the DSTO report (2014), as well as the need for greater clarity and effectiveness in partnerships and communication between Government and industry.

The increased focus on information sharing between the government and the private sector also occurred in the Unites States, with an executive order by President Obama in 2013 (Nakashima, 2014). This executive order mandated increased cyber threat information sharing between government agencies and the private sector to enhance their cyber resilience (Nakashima, 2014). The executive order was made in reaction to issues passing legislation proposing the implementation of cyber security standards to force greater information sharing between companies who own or manage critical infrastructure and the US Government (Nakashima, 2014). Across 2013, more than 3000 US companies were informed of cyber attacks on their systems by the FBI and Homeland security, many of those attacks suspected of being sponsored by China (Nakashima, 2014). The FBI reported that many of these companies were unaware of the breach, demonstrating the need for greater information sharing between the US Government and the private sector (Nakashima, 2014). The suspected increase in state-sponsored cyber attacks became a rising concern. In 2015, the US Director of National Intelligence expressed concerns that the next war wouldn't be physical

combat, but rather a cyber catastrophe (Austin and Slay, 2016a). This connection between cyber security and national security was further reinforced when then President Obama declared cyber security a national security emergency in 2016 and unveiled $26 billion to be spent over the year to introduce remedial policies to protect sectors outside of defence (Austin, 2016, Austin and Slay 2016b).

The 2016 Defence White Paper flags collaboration with industry and academia to counter cyber threats and increased collaboration with international partners, particularly the United States (Department of Defence, 2016). The White Paper also describes the enhancing the capability of the ACSC and increasing resilience of Defence networks as being central to strengthening Australia's cyber defences (Department of Defence, 2016**).** While Australia's budget of $100 million for implementation of the 2016 Cyber Security Strategy pales in comparison to the US' 2016 $26 billion and the UK's 2015 $800 million commitments (Austin and Slay 2016b), Australia's 2016 Cyber Security Strategy led to major changes and developments in Australia's cyber security infrastructure and security landscape. Particularly with the increased scope of the Australian Cyber Security Centre (ACSC) and the formation of the Joint Cyber Security Centre Initiative (JCSC).

3.2.2 The Australian Cyber Security Centre

The ACSC was announced in 2013 by then Prime Minister Julia Gillard to bring together expertise from across government agencies and co-locate them to improve response times to cyber incidents and facilitate a more comprehensive understanding of cyber threats to CI and government systems (Department of Defence, 2013). The ACSC was expected to be fully operational by the end of 2013 (Department of the Prime Minister and Cabinet, 2013), however it was officially opened in November 2014 (Department of the Prime Minister and Cabinet, 2014). It wasn't until 2015 that it became fully operational (Smith and Ingram, 2017). The ACSC sat within the Attorney-General's Department until July 2018, when the ACSC, CERT Australia and the Digital Transformation Agency were moved to the Department of Home Affairs (Portillo-Castro, 2019, Barker, 2018).

The ACSC was designed to become the backbone of Australia's cyber incident responses and to be a centralised location for the DSD (now ASD), ASIO, AFP, DIO, CERT Australia and the ACC (Department of the Prime Minister and Cabinet, 2013, Slocombe, 2013). To achieve this, the ACSC seconded staff from agencies such as the ASD, DIO, AFP, ASIS, ASIO and the Cyber Security Policy Division of the Department of Home Affairs (Australian Signals Directorate 2019d). The 2013 Defence White Paper flags Defence as having a leadership role in the ACSC due to the ACSC's national security importance and its role as the central national capability (Department of Defence, 2013). The 2016 Defence White Paper also acknowledges the role of the ACSC, citing it as a site of cooperation between Defence, the ASD and other agencies (Department of Defence, 2016).

To achieve this, the ACSC has three main roles; to analyse cyber threats cyber threats and uncover their nature and level of threat, to help protect Australia's essential networks and systems by collaborating with industry partners and the critical infrastructure sector, and provide advice on current and emerging threats (Department of the Prime Minister and Cabinet, 2013). The ACSC also fosters government collaboration with states and territories, broader industry and academia (Department of the Prime Minister and Cabinet, 2013, Pearce, 2018, Slocombe, 2013).

The ACSC developed a broad range of educational and collaborative programs designed to enhance cyber security across both government and industry (Australian Signals Directorate, 2019a, Department of the Prime Minister and Cabinet, 2013). For example, in November 2018 the ACSC ran a program to increase cyber resilience in the energy sector (Australian Signals Directorate, 2019a). 50 industry partners and government agencies participated in exercises including incident response training, exchange of operational technology expertise and red teaming (Australian Signals Directorate, 2019a). Through this program, the participants were able to share information about industry best practice and build towards enhancing cyber resilience (Australian Signals Directorate, 2019a).

In addition, the ACSC held annual cyber security conferences between 2015 and 2018 in Canberra designed for government and industry to share knowledge and best practice (Riley, 2019). Speakers at these conferences included international law enforcement agencies like the FBI, large Australian businesses like Telstra and Australia Post, and government speakers

such as Home Affairs Minister Peter Dutton (Riley, 2019). However, in 2019 the ACSC collaborated with the Australian Information Security Association rather than holding their own conference (Australian Information Security Association, 2019). Then Head of the ACSC Alastair MacGibbon argued that it is the responsibility of the cyber security industry to organise conferences (Stilgherrian, 2019). However, the ACSC would still be involved in conferences, giving presentations and holding smaller, more specialised events (Stilgherrian, 2019).

The ACSC also releases yearly threat reports designed to provide an overview of the threat landscape of the year before, including an overview of major threat actors, examples of incidents, types of threats and responses (ACSC, 2015). The report is compiled by the ACSC based on information provided by the industry and government partners of the ACSC and JCSC (ACSC, 2015). In this way, the ACSC is able to provide a more complete picture of Australia's cyber threat landscape and work to fill any knowledge gaps by leveraging the connections and expertise of the partner organisation, both government and industry (ACSC, 2015).

In 2016 the ACSC was moved to a purpose-built facility in Brindabella Business Park, in order to capitalise on the knowledge base and staff from the intelligence community and combine all expertise in one building (ACSC, 2017: 20). This allowed the ACSC to enable faster and more efficient communication of cyber threat information across the ACSC network (ACSC, 2017). It also helped to facilitate open and seamless communication between government and industry partners (ACSC, 2017).

In 2017, the Independent Intelligence Review recommended that the ACSC should "bring together all of the Government's cyber security capabilities" (Department of the Prime Minister and Cabinet, 2017: 65). To do this, all government agencies, especially the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) should increase their presence in the ACSC (Department of the Prime Minister and Cabinet, 2017). To achieve this goal, each agency should second staff to the ACSC, but the seconded staff should retain their access to the data and systems of their home agency (Department of the Prime Minister and Cabinet, 2017). By retaining access to their home agency's capability, the ACSC can leverage the information from each agency to provide a centralised and comprehensive response to cybercrime and cyber threats (Department of the

Prime Minister and Cabinet, 2017).

In July 2018, after the recommendation of the 2017 Independent Intelligence Review, the ASD became a statutory agency with its own legislative guidance within the Defence portfolio (Frewen, 2019, Kuper, 2018, Parliament of Australia, 2018). This reflects the ASD's increasing role in Australia's cyber security responses, including the ACSC becoming part of the ASD (Frewen, 2019, Parliament of Australia, 2018). This enabled the ASD to take a more proactive stance in cyber capability as well as maintain its original functions of supporting the ADF and combat predominant threats to Australia (Frewen, 2019, Parliament of Australia, 2018). The ASD works closely with the ACSC, with much of the ASD's partnerships occurring through the ACSC for both public partnerships and classified operations and intelligence purposes (Pearce, 2018). In order to facilitate partnerships between the Federal Government and private industry, the 2016 Cyber Security Strategy (2016) recommended the creation of Joint Cyber Security Centres to be located in major cities across Australia. The JCSCs are a vital part of the ACSC's Partnership Program designed to drive collaboration between industry and government to more effectively combat cyber threats (Australian Signals Directorate, 2019e).

3.2.3 The Joint Cyber Security Centre Initiative

The $47 million Joint Cyber Security Centre (JCSC) initiative was created under ACSC as part of the 2016 Cyber Security Strategy (Attorney-General's Department, 2017a, Barbaschow, 2017). It was designed to facilitate collaboration between the Federal Government and private industry in line with the strategic goals of the ACSC (Attorney-General's Department, 2017a, Kuper, 2018, Australian Signals Directorate, 2019e). To do this, JCSCs were opened in capital cities in each state except the Northern Territory and Tasmania in order to co-locate government and industry personnel (Attorney-General's Department, 2017a). The JCSC initiative currently has over 200 partner organisations across government, industry and academia (Australian Signals Directorate, 2019c).

The first JCSC was opened in Brisbane in February of 2017 (Barbaschow, 2017). Between the opening of the Brisbane JCSC in February 2017 and August of that year, the Brisbane JCSC registered 32 industry partners (Attorney-General's Department, 2017a). This includes

Telstra, Qantas, Rio Tinto and the Commonwealth Bank, showing the scale and range of participants in the JCSC and industry's acknowledgement that there as a need for this kind of collaborative organisation (Attorney-General's Department, 2017b). This, combined with interviews from JCSC partners in the JCSC monthly newsletters (Attorney-General's Department, 2017a), show that the JCSC initiative has value for private industry and fills a gap in Australia's cyber security responses.

The Melbourne JCSC opened eight months after Brisbane's JCSC in October 2017 and was expected to leverage the larger body of expertise in Melbourne (Spencer, 2017). Both the Melbourne and Brisbane JCSCs were led by CERT Australia as part of the Attorney-General's Department (Spencer, 2017). The Adelaide JCSC opened in November 2018, and was significant because some of Australia's most important defence, energy and infrastructure assets are in South Australia, thus making the JCSC particularly valuable for industry and government (Kuper, 2018). The Sydney JCSC opened in March 2018, with a capture the flag exercise between JCSC participants and a speech from founding partner IAG (CERT Australia, 2019a). The Perth JCSC opened in July 2018, and is significant because it brings together industries that represent a large percentage of Australia's gross domestic product (CERT Australia, 2019b). These include the mining sector, natural resources, agriculture, infrastructure and defence (CERT Australia, 2019b).

Business and government organisations that wish to be a part of the JCSC initiative must meet a set of criteria before being accepted into the JSCSC and ACSC (Attorney-General's Department, 2017a). Government departments that want to become a member of the JCSC must have an interest in or responsibility for cyber security (Attorney-General's Department, 2017a). This encourages participation from intelligence agencies and law enforcement (Attorney-General's Department, 2017a). In order to become an industry partner with the JCSC, a business must have an ABN, operational cyber security capability within Australia through an IT team or department, and must address areas of national interest, including critical infrastructure (Attorney-General's Department, 2017a). Smaller businesses with an ABN may participate through the JCSC's Online Portal (Attorney-General's Department, 2017a).

In 2017, there were strict guidelines for cyber security vendors and academics who wish to participate in the JCSCs (Attorney-General's Department, 2017a). Cyber security vendors

were limited to event-only participation, but consultancy firms were invited to participate more generally if they were volunteering their services (Attorney-General's Department, 2017a). Academics were only eligible to join the JCSC if their research specifically addressed information sharing, filling the cyber skills gap or if they were collaborating with JCSC partners on research projects in line with the JCSC's needs (Attorney-General's Department, 2017a). However, as of 2018, these limitations for security vendors were changed so that any security vendor willing to provide their cyber capability on a not-for-profit basis may become a member of the JCSC (Australian Signals Directorate, 2019d). Furthermore, the guidelines for academia, research and not-for-profits are much broader (Australian Signals Directorate, 2019d).

As with the JBFSIT, all partners must sign a non-disclosure agreement before being able to access JCSC and ACSC resources (Attorney-General's Department, 2017a). This both helps to protect the information shared by each party, but also encourages competitors to share information and best practice to enhance their cyber security capability and responses. Each member of the JCSC must contribute resources to the Centre based on the five objectives of the JCSC: education, information sharing, threat intelligence, development of solutions, and access to tools and practical resources (Attorney-General's Department, 2017a, Barker, 2018). This can be in the form of seconded staff on a full time or part time basis, staff on rotations or activity-based participation (Attorney-General's Department, 2017a). In addition to this, each partner is expected to contribute information to the JCSC and collaborate with other partners to improve responses to cyber threats and overall cyber security capability (Attorney-General's Department, 2017a).

3.2.4 Strategic Frameworks of ACSC and JCSC

As mentioned above, the ACSC was designed to become the backbone of Australia's cyber incident responses (Department of the Prime Minister and Cabinet, 2013). To achieve this, the ACSC has three main roles; to analyse cyber threats to uncover their nature and level of threat, to help protect Australia's essential networks and systems by collaborating with industry partners and the critical infrastructure sector, and provide advice on current and emerging threats (Department of the Prime Minister and Cabinet, 2013, Australian Signals Directorate, 2019c). The ACSC also provides workshops and educational campaigns to the

greater public (Australian Signals Directorate, 2019d). The ACSC also allows for government collaboration with states and territories, broader industry and academia (Department of the Prime Minister and Cabinet, 2013). To fulfil these roles, the ACSC has four key functions; analysis, collaboration and communication and research and development (Department of the Prime Minister and Cabinet, 2013).

The relationship between the ACSC and JCSCs is extremely close, with much of the literature discussing the JCSC through its contributions to the ACSC (Department of the Prime Minister and Cabinet, 2017, ACSC, 2017). The Government's contribution to the JCSCs is managed by CERT Australia, which until 2018 was part of the Attorney-General's Department (Department of the Prime Minister and Cabinet, 2017, CERT Australia, 2018). In 2018, CERT Australia moved to the ACSC, with staff moving across to the office in the Brindabella Business Park (CERT Australia, 2018).

The JCSC initiative has five objectives designed to help achieve the strategic goals of the ACSC (Attorney-General's Department, 2017a, Barker, 2018). First, to facilitate information sharing quickly across JCSC partners (Attorney-General's Department, 2017a, Barker, 2018). This includes threat intelligence, sensitive information and incident intelligence (Attorney-General's Department, 2017a, Spencer, 2017). The second objective is to develop responses and solutions to cyber threats and risks through collaboration between JCSC partners, including State and Federal Governments (Barker, 2018, Attorney-General's Department, 2017a). Third, the JCSCs aim to provide a comprehensive understanding of Australia's cyber threat landscape through information sharing and threat analysis (Attorney-General's Department, 2017a, Barker, 2018). The fourth objective of the JCSCs is to provide practical tools and resources to improve cyber security (Attorney-General's Department, 2017a, Barker, 2018). These tools and resources would be made accessible to all partner organisations of the JCSCs (Attorney-General's Department, 2017a). Finally, the JCSCs provide education and information to partners through workshops and newsletters led by each centre (Attorney-General's Department, 2017a, Barker, 2018).

3.2.5 Strengths and Weaknesses of the JCSC

The JCSC initiative is a public-private partnership (PPP), bringing together expertise from

different industries including banks, airlines and tech companies, as well as State and Federal law enforcement agencies and government departments. This large mix of partners allows the JCSCs to compile a more comprehensive threat matrix (ACSC, 2017). It also facilitates a greater understanding of the threats facing Australian businesses of all sizes, and helps Australian based businesses see the impact of cyber threats and attacks across the globe. This is one of the key advantages of the PPP model for both government and industry (Christensen and Petersen, 2017). By combining resources, it is possible to leverage different knowledge, specialities, and capability to combat cyber threats, enhance knowledge of the threat landscape and develop solutions, all of which are vital to the JCSC's purpose.

The large variety of industries involved in the JCSCs also encourages innovation between industries. With different industries facing similar threats, businesses can draw inspiration from the actions and perspectives of others, which can inspire creative solutions through communication and an understanding of how other businesses are combatting cyber threats. Furthermore, the JCSC encourages teamwork and collaboration across industry and government to capitalise on the range of skills and knowledge to create solutions and management strategies for cyber threats (Australian Signals Directorate, 2019d, Henderson, 2018).

Another strength of the JCSC is that it is open to businesses of all sizes, making the information and intelligence available for all businesses who wish to take part in the JCSC (Australian Signals Directorate, 2019e). As discussed above, there are two main conditions for membership of the JCSCs. First, each company must sign non-disclosure agreement before being allowed access to the JCSC resources (Attorney-General's Department, 2017a). Second, each business must provide resources to the JCSC, they cannot just benefit from the JCSC's work, they must also be active participants in the information and capability sharing (Attorney-General's Department, 2017a). This ensures that each participant of the JCSC contributes to the overall efficacy of the JCSC as well as provide valuable information to help improve the JCSC's responses to cyber incidents.

Furthermore, the information brought to the JCSCs is combined with the broader knowledge from the ACSC and compiled into a yearly threat report (ACSC website, 2017 Threat report). These threat reports are publicly available and free to access, and provide an overview of Australia's threat landscape. Without the information from the JCSC, the ACSC Threat

Reports would not be as informative or comprehensive (ACSC, 2017). The information collected as part of the JCSC initiative also helps the JCSCs and ACSC to put together events to address the needs of the JCSC partners (Australian Signals Directorate, 2019e). For example, in 2019 alone the JCSCs in each state have held drop-in days for partner organisations, specialised workshops for law enforcement agencies, and talks from companies such as IAG Insurance and the Red Cross (Australian Signals Directorate, 2019e). These examples show the broad range of events that the JCSC and ACSC provide to their partner organisations to enhance cyber resilience and cyber security across all partners.

As the JCSC initiative is still in its infancy and has close ties to the ACSC and ASD, it is difficult to find crucial independent evaluation of the JCSC initiative. This would be an important area for further research as more progress reports, Hansards and discussion papers are released in the future. Despite this, there are some weaknesses in the JCSC initiative that have emerged. First is in its lack of definable impact, it is difficult to find evaluation of the JCSC initiative's outcomes and how successful it is in reaching its goals (GAP Taskforce on Cyber Security, 2017). The operational connection between the JCSCs and law enforcement is not clear, making it difficult to examine how information is transferred between the ACSC, JCSC and law enforcement bodies for operational purposes. While there are reports from operations and investigations undertaken, such as Operation Manic Menagerie, the operational processes and referral processes are not clear (Australian Signals Directorate, 2019f, ACSC, 2018). This makes it difficult to evaluate the success of the JCSC initiative.

While one of the key strengths of the JCSC initiative is its ability to combine industry and government knowledge in a public-private partnership (PPP), the effectiveness of the PPP model relies on the clear defining of roles and responsibilities between the parties (Christensen and Petersen, 2017). In the case of the JCSC initiative, the GAP Report identifies that the roles of the JCSC and its partners were not clear enough, leaving ambiguity and differing expectations of who leads the collaboration (GAP Taskforce on Cyber Security, 2017). Therefore, while industry and government both advocated for collaboration, they expected the other party to tale the leading role (GAP Taskforce on Cyber Security, 2017).

In addition, with the ASD working closely with the ACSC (Pearce, 2018, Australian Signals Directorate, 2019e), the JCSCs take on more importance for industry partners that may not want such a close connection with the ASD. By signing strict non-disclosure agreements, the

JCSCs provide the ASD with more information, and industry access to the JCSC information network, without the close connection with the ASD. By providing businesses with a space to share experience, best practice and intelligence, the JCSC is valuable for both industry and government (Attorney-General's Department, 2017a). However, there are still risks associated with close government influence (Carr, 2016, Christensen and Petersen, 2017). While the JCSC is a PPP, it still answers to the ACSC which is part of the ASD which has a heavy focus on concerns around national security. This may increase the risk that information from the JCSC initiative could be used in ways the individual participants have not consented to.

Another weakness of the JCSC, particularly for the Federal Government is that the JCSC initiative is not compulsory for the critical infrastructure sector or State and Federal Government Departments. For example, the Western Australian Parliament asked all government departments whether they were a part of the JCSC initiative, and why not (if eligible) (Parliament of Western Australia, 2018). What they found was that while most of the eligible departments were members, some departments like the Electoral Commission chose not to participate in the JCSC initiative, judging their own cyber security measures adequate (Parliament of Western Australia, 2018). This decision by the Western Australian Electoral Commission was after the use of system iVote in the 2017 state elections, despite iVote's previous security vulnerabilities and a lack of oversight from the Western Australian Government (Culnane et al., 2017). This shows that without mandatory participation in the JCSC initiative, it is more difficult to minimise vulnerabilities and create the holistic and comprehensive network that the JCSCs aim to provide. Furthermore, it means that government departments cannot access the information network, tools and training that the JCSC provides to partners.

3.2.6 Cyber Security Beyond 2019

The 2020 Cyber Security Strategy Discussion Paper (2019) has been released by the Department of Home Affairs in preparation for the release of a 2020 Cyber Security Strategy. The discussion paper outlines how the 2016 Cyber Security Strategy has been implemented, and the changes in priorities for the Federal Government (Department of Home Affairs, 2019). Furthermore, the discussion paper identifies the changes in cyber threats facing Australians between 2016 and 2019, and looks to the challenges the future may bring

(Department of Home Affairs, 2019). In particular, the discussion paper identifies the rising threat from state actors in cyberspace after high profile cyber attacks were attributed to state actors in 2019, and the importance of securing Australia's critical infrastructure (Department of Home Affairs, 2019).

The role and responsibilities of the ACSC are increasing, with cyber 'sprint teams' created under the ACSC in 2019, in addition to the release of the Information Security Manual and Essential Eight strategies for cyber incident mitigation (Pearce, 2019, Reichert, 2019). The 2020 Cyber Security Strategy Discussion Paper also identifies the ACSC as being vital to Australia's cyber security strategy, and the role of the ASD is reinforced with discussions of expanding the ASD's capability (Department of Home Affairs, 2019). The JCSC initiative is also flagged for further expansion, with video conferencing capability being arranged between Tasmania and the Northern Territory to help partners access ACSC workshops and events (Department of Home Affairs, 2019).

Other Government Departments are also in the process of revising their cyber security strategies including the Department of Human Services (2019), the Office of the Australian Information Commissioner (Braue, 2019) and the South Australian Government (2019) in line with the changing cyber threat landscape. These changes show the ever increasing risk of cyber attacks and how organisations are responding to the changing threat landscape. For the Federal Government, the ASD and ACSC remain essential to Australia's cyber security and ensuring the protection of critical infrastructure and national security. The JCSCs play an important role in enhancing collaboration between private industry and government, a role which remains essential for both the ACSC and ASD.

3.2.7 Conclusion

The JCSC initiative under the ACSC has been instrumental in helping the ACSC achieve its strategic goals by fostering collaboration between government agencies and departments and private industry. By opening centres across five of Australia's largest cities, the JCSC initiative provides a forum for JCSC partners to attend workshops, collaborate and share information quickly and effectively. The JCSC initiative then feeds back into the ACSC, providing threat information and encouraging collaboration with Australia's intelligence

community.

The next chapter will contain a comparative analysis of the JBFSIT and the JCSC to examine the similarities and differences in strategic goals, formation, parent organisation, and how they fit into Australia's security landscape. This will show that both organisations have very similar goals, and the key difference between them is in the way they reflect the strategic priorities of the Federal government at that time.

3.3 Comparative Analysis

This section will provide a comparative analysis of the Joint Banking and Finance Sector Investigations Team and the Joint Cyber Security Centre initiative. While the time difference between these case studies span more than 10 years, there are clear similarities between them. This section will compare the goals of the Australian High Tech Crime Centre (AHTCC) and the Australian Cyber Security Centre (ACSC), as well as the Joint Banking and Finance Sector Investigations Team (JBFSIT) and the Joint Cyber Security Centre Initiative (JCSC). This will show that despite the small differences in scope and speciality, the biggest difference between these Government-sponsored responses to cyber threats lies in the language and framing of these cyber security responses.

3.3.1 Goals of the AHTCC and ACSC

As argued in Chapter Two, discourses around cyber security have changed significantly between 2000 and 2019, which is very clear when comparing the goals of the AHTCC with the ACSC and the JBFSIT with the JCSC initiative. The below table compares the core goals of the AHTCC with those of the ACSC. Fundamentally, the AHTCC and ACSC have the same goals, as summarised in the table below. The major difference between the AHTCC and ACSC's goals is in the language through which the goals are expressed.

AHTCC	ACSC	Summary
To provide a centralised approach to technology enabled crime (AHTCC, 2008a, Platypus, 2009)	To be the central location for Australia's cyber security capability (ACSC, 2017)	Centralise cyber capability
Assisted in improving the ability to manage technology enabled crime across all jurisdictions (AHTCC, 2008a, Platypus, 2009)	Provide advice on current and emerging threats to enhance overall cyber security (ACSC, 2017)	Provide threat intelligence and enhance cyber resilience
Supported the protection of the National Information Infrastructure (NII) (AHTCC, 2008a, Platypus, 2009)	Help protect Australia's essential networks and systems by collaborating with industry partners and the critical infrastructure (CI) sector (ACSC, 2017)	To protect essential services and industries

N/A	Analyse cyber threats to uncover their nature and level of threat (ACSC, 2017)	Analyse cyber threats and rank their level of threat

Table 1: Goals of the AHTCC and the ACSC

The AHTCC's goals are framed through a policing lens, with terms such as 'technology enabled crime' and the 'National Information Structure'. This is a different set of terminology to what appears in the ACSC documentation, with terms such as 'Critical Infrastructure' and 'Cyber Security'. These terms are used to represent the evolution of cyber threats shifting from a policing framework through the AFP and AHTCC to a Defence and national security framework through the ACSC and the ASD.

3.3.2 Goals of the JBFSIT and JCSC

The JBFSIT and JCSC initiative were both created to further the strategic goals of their parent organisation, the AHTCC and ACSC respectively, as discussed in the above section. In order to do this, both organisations have four main objectives. The table below shows the four goals of the JBFSIT and the JCSC initiative side-by-side. What this table shows is that while the goals of the JBFSIT are more specific to the banking sector, three out of the four goals of the JBFSIT and JCSC initiative address the same concerns. The exception to this is in the JBFSIT's focus on intelligence gathering to support law enforcement operations and provide evidence to lead to prosecutions (AHTCC, 2006). The JCSC initiative however, has the goal of providing practical tools and resources to partners of the JCSC (Attorney-General's Department, 2017a).

JBFSIT	JCSC	Summary
Foster collaboration and information sharing with the private and public sectors (AHTCC, 2006, McKenzie, 2006)	Facilitate information sharing quickly across JCSC partners (Attorney-General's Department, 2017a, Barker, 2018)	Collaboration and information sharing in a PPP
N/A	Provide practical tools and resources to improve overall cyber security	Provide practical tools and resources

	(Attorney-General's Department, 2017a, Barker, 2018)	
Provide intelligence assessments based on information from the banking sector (Parliament of Australia, 2006a)	Provide education and information to partners through workshops and newsletters (Attorney-General's Department, 2017a, Barker, 2018)	Educate partners about current and emerging threats
Design and implement measures to minimise, mitigate the impacts of financial fraud (AHTCC, 2006, McKenzie, 2006)	Develop responses and solutions to cyber threats and risks (Attorney-General's Department, 2017a, Barker, 2018)	Develop responses and solutions to cyber incidents and threats
Provide evidence to lead to successful prosecution of financial fraud, including identification of people involved in malicious activity (AHTCC, 2006, McKenzie, 2006)	N/A	Provide evidence to facilitate prosecution

Table 2: Goals of the JBFSIT and the JCSC initiative

One of the key strengths for both the JBFSIT and the JCSC initiative is encapsulated in the first goal of the case studies; to foster collaboration and information sharing across the JBFSIT and JCSC initiative partners. Both the JBFSIT and the JCSC initiative are public-private partnerships (PPPs) designed to leverage the capability of the public and private sectors in order to combat shared threats. The JBFSIT was one of the world's first PPPs and presented a new way of negotiating the competing interests of the Federal Government and the banking sector while maximising intelligence and operational output (Platypus, 2009). The JCSC initiative provides the opportunity for organisations within the critical infrastructure sector and national security sector to engage in a mutually beneficial partnership (Attorney-General's Department, 2017a).

PPPs have the advantage of providing access to different bodies of knowledge and the opportunity to leverage capabilities and information that would not otherwise be available (Carr, 2016). For both the JBFSIT and the JCSC, the PPP arrangement allows for the government departments and industry to share their experience, best practice and issues they are facing within their own businesses. Furthermore, it provides the opportunity for to collaborate and develop strategies to mitigate the impacts of cyber attacks and cyber threats, and shares the cost across all parties (Carr, 2016). In this way, the JBFSIT and JCSC perform

a similar role for industry by providing the platform for collaboration and information sharing.

The second common goal for the JBFSIT and the JCSC is in educating partners about current and emerging threats. While it was a later addition to the JBFSIT's role, collecting monthly information on cyber threats from the banking sector and distributing a summary to all JBFSIT partners became a major part of the JBFSIT's role (Parliament of Australia, 2006a). This helped to create an information network between the JBFSIT partners and facilitated the information sharing process. It also maintained the incentive for the banks to report honestly on their progress, something that was difficult to measure before the JBFSIT (McKenzie, 2006). The banking sector were reluctant to provide information to law enforcement, especially in reporting cyber incidents due to the lack of incentive to report and the risk of jeopardising consumer confidence (McKenzie, 2006). One of the JCSC's greatest strengths is its focus on education and training. The JCSC initiative, in collaboration with the ACSC hold regular education and training events, both specialised events and general cyber security training (Australian Signals Directorate, 2019e). The goal of this training is to enhance Australia's overall cyber resilience and cyber security (Australian Signals Directorate, 2019e). While the JBFSIT's education newsletters were limited to the banking sector, the JCSCs provide education and information to a broader range of partners with varying levels of participation via the JCSC websites, newsletters and ACSC Threat Reports.

The third shared goal of the JBFSIT and JCSC initiative is the development of strategies to manage the cyber threats facing each case study. The PPP arrangement of the JBFSIT brought together companies that would normally be in competition, and encouraged them to work together and with law enforcement, particularly the AFP to design and implement measures to respond to the rise in phishing scams and financial fraud (McKenzie, 2006). In the JCSC initiative, partners work together to design a range of measures to combat cyber threats facing the critical infrastructure and security sectors. This includes activities such as the capture the flag exercise held at the JCSC opening in Sydney, simulations and threat sharing activities.

3.3.3 Achieving These Goals

The AHTCC website defines the five functions through which the AHTCC fulfils the goals shown in the table above (AHTCC, 2006). These are; coordination, investigation, intelligence, liaison and knowledge (AHTCC, 2006). I argue that these functions are applicable not only to achieving the AHTCC's goals but also the ACSC's goals and they provide a good framework to compare the JBFSIT and JCSC initiative's goals.

As discussed in Chapter 3, coordination refers to the coordination between Australian law enforcement, international agencies and the Federal Government about cybercrime (AHTC, 2006). Investigation refers to investigations conducted by the AHTCC or referred to partner agencies (AHTCC, 2006). Intelligence refers to knowledge and programs that enhance knowledge of the cyber threat landscape (AHTCC, 2006). Liaison refers to communication and cooperation with industry and government including policy, business, technical and investigative cybercrime issues. Finally, knowledge refers to knowledge of best practice, preventative measures, training and education, and expert advice (AHTCC, 2006).

While the goals of the JBFSIT focus on the banking sector and its partnership with law enforcement, and the JCSC's goals focus on increasing general cyber security across its partners in different industries, both conform to the five functions defined by the AHTCC. In fostering collaboration and information sharing, both the JBFSIT and the JCSC coordinate with law enforcement and other partners and add knowledge to the threat landscape. While both the JBFSIT and the JCSC share intelligence, the JCSC initiative specifically aims to provide up-to-date information through its five centres, online information sharing portal and the ACSC's 24/7 hotline (ACSC, 2017). This is in contrast to the JBFSIT, where information was collected, collated and made available to its members monthly unless otherwise requested, such as in the case of a cyber incident (McKenzie, 2006).

In educating partner organisations about current and emerging threats, the JBFSIT and JCSC liaise with government and other partners and conduct training and education to leverage knowledge in order to provide information about best practice and training. Again, the JCSC's education and training programs are much more extensive then the JBFSIT's programs. This is partly due to the difference in funding, with the JCSCs funding of $47 million Attorney-General's Department, 2017a, Barbaschow, 2017). It could also be

explained by the broad range of partners involved in the JCSC and its focus on training, as discussed in Chapter 4. The JCSC initiative's five centres as opposed to the two centres of the JBFSIT could also explain the broader range of training and resources.

Finally, the JBFSIT and JCSC leverage intelligence provided by partners, and knowledge generated through collaboration to developing solutions to incidents and threats. The development of these solutions and strategies may also include coordination with law enforcement through referrals of information to the relevant law enforcement agency, such as in the JBFSIT. It may also include liaising with other industry and government partners to share information on best practice and provide access to practical tools and resources, which the JCSC provides.

The similarities between the JCSC and JBFSIT could also reflect their common leadership. Alastair MacGibbon has been an influential figure in shaping Australia's cyber security policy through various government roles including as the eSafety Commissioner (Donaldson, 2019). MacGibbon was the Head of the AHTCC from its establishment, thereby giving him significant input into the running and foundation of the AHTCC. After leaving the AHTCC and the government sector in 2004, MacGibbon returned as the eSafety Commissioner in 2015 (Donaldson, 2019). Beyond his role as the Special Adviser on Cyber Security MacGibbon became the Head of the ACSC when it moved to the ASD in 2018 (Donaldson, 2019). While the JCSCs opened through 2017 and 2018, MacGibbon as head of the ACSC and with oversight of the JCSC initiative would still have been a driving force and influencing factor on both organisations.

3.3.4 Conclusion

Framing the discussion of the goals of the JBFSIT and JCSC through the AHTCC's five functions demonstrates how, despite their difference in focus, the JBFSIT and the JCSC were created for similar purposes and engage with the same functions in order to achieve their goals. These goals then help the AHTCC and ACSC achieve their strategic objectives, which the analysis above has shown are very similar, with the language being the key difference. This helps show the impact of the shift in discourse from that of e-crime and technology enabled crime, to national security and critical infrastructure. This reflects the shift in strategic

priorities of the Australian Federal Government in terms of cyber security, and what they believe are the most important and impactful threats.

More than ten years after the creation of the JBFSIT, the JCSC has elaborated on the same public-private (PPP) model with a broader scope, more funding, more resources and a closer connection to Australia's intelligence community. This demonstrates the important of PPPs for Australia's cyber security and provides further evidence for the JBFSIT's success, given the similarities between the JBFSIT and the JCSC initiative as well as the AHTCC and the ACSC. With a similar model and parallel goals, the JBFSIT and the JCSC initiative show how discourses around cyber security have changed from that of a policing framework to a national security framework

4. Conclusions

4.1 Summary of Findings

An analysis of the Australian Federal Government's cyber security policies, including Defence White Papers, Cyber Security Strategies and Independent Intelligence Reviews has shown that discourses around cyber security have changed significantly between 2000 and 2019. This discursive shift has seen cyber security move from a policing framework with terms like 'technology enabled crime' to a national security framework with terms like 'cyber warfare' becoming increasingly popular. These policies provide the Australian Government, Australian public and the international community with an outline of the Federal Government's strategic priorities around cyber security. As such, these policies and the language within reflect the Federal Government's responses to cyber threats. This is demonstrated through a comparative analysis of two case studies; the Joint Banking and Finance Sector Investigations Team (JBFSIT) and the Joint Cyber Security (JCSC) initiative. Together, these case studies show how the shift in discourse from that of a policing framework with the JBFSIT, to a national security framework with the JCSC initiative, influences Australia's law enforcement and national security communities in line with the language shift in these policies.

The Joint Banking and Finance Sector Investigations Team was created in 2004 under the Australian High Tech Crime Centre (AHTCC) within the Australian Federal Police (AFP). This was one of Australia's first public-private partnerships designed to combat financial crime. While it had no operational capability, the JBFSIT facilitated information sharing between law enforcement and the banking sector and encouraged collaboration between market competitors to find the best ways to manage financial crime. In 2008 the AHTCC and JBFSIT became part of the Australian High-Tech Crime Operations division of the AFP, combining operational and intelligence capability and combining the JBFSIT's specialist information with organised crime, terrorism and child exploitation units.

The JCSC initiative was created under the Australian Cyber Security Centre (ACSC) to facilitate collaboration between industry partners and the Federal Government. It did this through the establishment of JCSCs across five of Australia's largest cities between 2017 and 2018. These centres were designed to become hubs for partners to share threat information,

develop solutions to cyber attacks and cyber incidents, as well as a place for education and training for JCSC partners. The ACSC was originally part of the Attorney-General's Department, but moved to the Australian Signals directorate in 2018.

Fundamentally, the JBFSIT and JCSC share the same primary goal; to facilitate information sharing and develop solutions to the cybercrime priorities, as outlined by the Federal Government and in response to activities within Australia's threat landscape. The key difference between these two organisations is the way that cyber security has been framed. The language used in the two documents that proposed the creation of these organisations is radically different. For the JBFSIT, the dramatic rise in phishing scams in 2004 affected banks around the world, and the transnational nature of phishing scams meant that a new approach to financial crime needed to be implemented. This was approached from a policing framework, with communication and intelligence from the banking sector combined with the AFP. The JCSC however, developed in response to a rise in attacks and threats against critical infrastructure and government systems, and as part of the Federal Government's 2016 Cyber Security Strategy, which made a connection between cyber threats and national security concerns. This led to major changes across Australia's intelligence community and a call for increased collaboration between government and industry to manage these threats.

4.2 Broader Implications of this Research

4.2.1 Further Research

This thesis traces a shift in discourses around cyber security, from that of a cybercrime focus to that of a cyber warfare focus across publicly available official Federal Government policies. To understand the process through which the discourse shifted, it would be beneficial to interview staff from both the JBFSIT and JCSC initiatives to gain further insight into the evolution of these organisations. As discussed in Chapter 1, while this thesis traces the discursive shift, it did not attempt to explain why this shift took place. Further research into this aspect would help to provide a more comprehensive understanding of the evolution of Australia's cyber security priorities and how they impact government-sponsored action.

This thesis compares two case studies, one from 2004 and the other from 2017-2018. The examination of the evolution of Australia's response to cyberthreats could be further enriched

with additional case studies. This would be particularly relevant for the comparatively recent JCSC initiative, whose work and effects are yet to be comprehensively explored in academia and public media due to the security classification of much of the information. With more time, the impact of the JCSCs will become clearer, which will provide further evidence for the arguments made in this thesis and for further research into private-public partnerships in Australia and their value.

Another avenue for future research would be an examination of the impact of the shift in discourse on private industry in Australia, to demonstrate the impact of government policies on private industry priorities. Furthermore, research could be undertaken to examine the influence of private industry and technological advances on the formation of the official government policies to examine the relationship between private industry and the Federal Government. This would also provide insight into how these policies are created and what outside factors help shape the Federal Government's strategic priorities.

Furthermore, it would be valuable to compare the shift in discourses in Australia to those internationally, particularly with the other Five Eyes countries. This comparison would allow for researchers to consider the global trajectory of cyber capability and to see whether these countries have seen the same shift in discourses and the implications for their security landscapes. Furthermore, this research would allow for connections to be observed between the countries as discover whether there were common events or technological developments that encouraged the shift from discussions of cybercrime to discussions of cyber warfare. The rise of cyber security discourse in Australia and other Western countries could also be compared with global powers China and Russia, who have developed their own cyber warfare capabilities and see whether there are any commonalities or major points of difference.

Finally, this thesis focused on Australian Federal Government official policies on a strategic and government level. Further research would be needed to examine the changes that have occurred through this time in the Australian Defence Force. Discussions of the Australian Defence Force policies and capability development could not fit within the limitations of this project, however Defence has been a driver of innovation and technological developments across 2000-2019. The ADF has also seen major changes based on the shift from cybercrime discourse to that of cyber warfare, particularly in research and jurisdiction. Further research

into the changes undertaken by the ADF could provide further evidence for the arguments made in this thesis.

4.2.2 Implications for Australia's Future Cyber Policies

Discourses around cyber security are likely to continue to shift, with each policy adapting to the evolving threat landscape and technological developments including threats and vulnerabilities emerging from the Internet of Things and a continuing rise in state activity in cyberspace. The 2020 Cyber Security Strategy Discussion Paper released by the Department of Home Affairs calls for submissions from the public as to how the Australian Government can better manage Australia's cyber security directives. It also outlines some of the key priorities for the Government moving forward. In particular, the discussion paper identifies national security, the ACSC, the JCSC initiative and the Australian Signals Directorate (ASD) as being vital to Australia's cyber resilience and cyber capability. Also discussed is the rising threat of state-sponsored cyber attacks and developing cyber capability as being important parts of Australia's cyber security strategy in the future.

The Australian Federal Government's public cyber security and defence policies outline the Government's strategic priorities for cyber security. The shift in language from a policing framework to a national security framework is evident in the law enforcement responses that have developed out of these policies. This demonstrates that the language used in the Federal Government's policies has a measurable impact on the Government's law enforcement responses initiatives, taskforces and programs.

5. Reference List

Admin. (2017). *Attorney-General Speech – Launch of Joint Cyber Security Centre Brisbane.* Available: https://australiansecuritymagazine.com.au/attorney-general-speech-launch-of-joint-cyber-security-centre-brisbane/. Last accessed 21 March 2019.

Accenture. (2019). *Future Cyber Threats: Extreme but Plausible Threat Scenarios in Financial Services*. Available: https://www.accenture.com/_acnmedia/pdf-100/accenture_fs_threat-report_approved.pdf. Last accessed: 14 October 2019.

Attorney-General's Department. (2009). *Cyber Security Strategy.* Canberra: Australian Government Publishing Service.

Attorney-General's Department. (2017a). *Newsletter: Joint Cyber Security Centre.* Issue 1: August 2017. Available at: https://webarchive.nla.gov.au/awa/20190305222729/https://www.cert.gov.au/jcsc/news

Attorney-General's Department. (2017b). *Launch of the joint Cyber Security Centre Pilot, Brisbane.* Available: https://webarchive.nla.gov.au/awa/20170303183657/https://www.attorneygeneral.gov.au/Speeches/Pages/2017/FirstQuarter/Launch-of-the-joint-cyber-security-centre-pilot.aspx. Last accessed 8 October 2019.

Attorney-General's Department. (2018). *Perth Joint Cyber Security Centre protecting West Australians.* Available: https://www.attorneygeneral.gov.au/Media/Pages/perth-joint-cyber-security-centre-protecting-west-australians-6-july-2018.aspx. Last accessed 21 March 2019.

AusCERT. (2019). *About AusCERT.* Available: https://www.auscert.org.au/about/. Last accessed 28 March.

Austin, G. (2016). *Australia Rearmed! Future Needs for Cyber-Enabled Warfare*. ACCS Discussion Paper 1: January 2016. Available at: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/DISCUSSION%20PAPER%20AUSTRALIA%20REARMED.pdf

Austin, G. (2018). *Cybersecurity in China: The Next Wave*. Cham: Springer International Publishing.

Austin, G. and Slay, J. (2016a). *Australia's Response to Advanced Technology Threats: An Agenda for the Next Government.* Australian Centre for Cyber Security UNSW Canberra. Available at: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/ADVANCED%20TECHNOLOGY%20THREATS%20AND%20AUSTRALIA%2030%20May%202106mediaversion.pdf

Austin, G. and Slay, J. (2016b). *The Australian government must take cyber security more seriously.* Available: https://theconversation.com/the-australian-government-must-take-cyber-security-more-seriously-60231. Last accessed 8 October 2019.

Australian Cyber Security Centre. (2015). *ACSC 2015 Threat Report.* Canberra. Available at: https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2015.pdf

Australian Cyber Security Centre. (2017). *ACSC 2017 Threat Report.* Canberra. Available at: https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2017.pdf

Australian Cyber Security Centre. (2018). Manic Menagerie: Malicious activity targeting web hosting providers: ACSC Report 2018-143. Canberra. Available at: https://www.cyber.gov.au/sites/default/files/2019-03/report_manic_menagerie.pdf

Australian Cyber Security Centre. (2019). *About the Australian Cyber Security Centre.* Available: https://www.acsc.gov.au/about.html. Last accessed 21 March 2019.

Australian Federal Police. (2004). *Australian Federal Police Annual Report 2003-2004.* Commonwealth of Australia: Canberra. Available at: https://www.righttoknow.org.au/request/4043/response/10684/attach/5/afp%20annual%20report%202003%202004.pdf

Australian Federal Police. (2009). *Australian Federal Police Annual Report 2008-2009.* Comonwealth of Australia: Canberra. Available at: https://www.righttoknow.org.au/request/4043/response/10685/attach/5/afp%20annual%20report%202008%202009.pdf

Australian Government. (2016). *Australia's Cyber Security Strategy: Enabling Innovation, Growth and Prosperity*. Canberra: Commonwealth of Australia.

Australian Government. (2017). *Australia's Cyber Security Strategy: 2017 Update.* Commonwealth of Australia. Available at: https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/cyber-security-strategy-first-annual-update-2017.pdf

Australian Government. (2017). *Australia's Cyber Security Strategy: 2017 Update.* Commonwealth of Australia. Available at: https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/cyber-security-strategy-first-annual-update-2017.pdf

Australian High Tech Crime Centre. (2004a). Media Release: Thursday, 28 August 2003. Available: https://web.archive.org/web/20041118085257/http://www.ahtcc.gov.au/. Last accessed 13 October 2019.

Australian High Tech Crime Centre. (2004b). What is the Australian High Tech Crime Centre <AHTCC>? Available: https://web.archive.org/web/20041118085257/http://www.ahtcc.gov.au/. Last accessed 13 October 2019.

Australian High Tech Crime Centre. (2004c). Allied organisations. Available: https://web.archive.org/web/20041118085257/http://www.ahtcc.gov.au/. Last accessed 13 October 2019.

Australian High Tech Crime Centre. (2006). *JBFSIT.* Available: https://webarchive.nla.gov.au/awa/20060820051806/http://www.ahtcc.gov.au/about_us/jbfsit. Last accessed 13 October 2019.

Australian High Tech Crime Centre. (2008a). *About Us.* Available: http://pandora.nla.gov.au/pan/39350/20081218-0000/www.ahtcc.gov.au/about_us/index-2.html. Last accessed 3 September 2019.

Australian High Tech Crime Centre. (2008b). Joint Banking and Finance Sector Investigations Team (JBFSIT) expands into Melbourne. [Press release], August. Available at: http://pandora.nla.gov.au/pan/39350/20081218-0000/www.ahtcc.gov.au/news_and_information/media_releases/JBFSIT_Melb.pdf

Australian Information Security Association. (2019). *ACSC and AISA seal partnership deal for a secure cyber future.* Available: https://www.aisa.org.au/Public/News_and_Media/News/ACSC%20and%20AISA%20seal%20partnership%20deal%20for%20a%20secure%20cyber%20future.aspx . Last accessed 8 October 2019.

Australian Signals Directorate. (2019a). *Electricity program generates a buzz.* Available: https://www.cyber.gov.au/news/electricity-program-generates-buzz. Last accessed 8 October

2019.

Australian Signals Directorate. (2019b). *Cyber security.* Available: https://www.asd.gov.au/cyber. Last accessed 8 October 2019.

Australian Signals Directorate. (2019c). *About.* Available: https://www.cyber.gov.au/about. Last accessed 8 October 2019.

Australian Signals Directorate. (2019c). *Business: JCSC Partners.* Available: https://cyber.gov.au/business/programs/jcsc-partners/ . Last accessed 21 March 2019.

Australian Signals Directorate. (2019d). *Joint Cyber Security Centres.* Available: https://www.cyber.gov.au/programs/joint-cyber-security-centres. Last accessed 8 October 2019.

Australian Signals Directorate. (2019e). *ACSC program enters its next phase through JCSCs.* Available: https://www.cyber.gov.au/news/acsc-partnership-program. Last accessed 8 October 2019.

Australian Signals Directorate. (2019f). *ACSC counters threat to web hosting providers.* Available: https://www.cyber.gov.au/news/manic-menagerie. Last accessed 8 October 2019.

Bajkowski, J. (2004a). *Banks' Phishing Cops Get Hi-Tech Crime Schooling.* Available: https://www.computerworld.com.au/article/128974/banks_phishing_cops_get_hi-tech_crime_schooling_/. Last accessed 25 August 2019.

Bajkowski, J. (2004b). *Exit Interview: Alastair MacGibbon, Director, Australian High Tech Crime Centre.* Available: https://www.computerworld.com.au/article/16193/exit_interview_alastair_macgibbon_direct

or_australian_high_tech_crime_centre/. Last accessed 25 August 2019.

Bajkowski, J. (2004c). *Exit Interview: AHTCC Director Alastair MacGibbon.* Available: https://www.cso.com.au/article/16194/exit_interview_ahtcc_director_alastair_macgibbon_/. Last accessed 27 August 2019.

Ball, D. and Waters, G. (2013). Cyber Defence and Warfare. *Security Challenges*. 9 (2), 91-98.

Balzacq, T. (2010). Constructivism and Securitisation Studies. In: Cavelty, M.D. and Mauer, V. *The Routledge Handbook of Security Studies*. New York and London: Routledge. 56-72.

Barbaschow, A. (2017). *Government launches first of AU$47m Joint Cyber Security Centres in Brisbane.* Available: https://www.zdnet.com/article/government-launches-first-of-au47m-joint-cyber-security-centres-in-brisbane/. Last accessed 8 October 2019.

Barker, S. (2018). *Sydney's Joint Cyber Security Centre opens in Darling Park.* Available: https://securitybrief.com.au/story/sydneys-joint-cyber-security-centre-opens-darling-park. Last accessed 8 October 2019.

Barnard-Wills, D. and Ashenden, D. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture*. 15 (2), 110 –123.

Bayuk, J. L., Healey, J., Rohmeyer, R., Sachs, M.H., Schmidt, J. and Weiss, J (2012). *Cyber Security Policy Guidebook*. United States and Canada: John Wiley & Sons.

Braue, D. (2019). *Government rewriting cybersecurity conversations around consumer focus.* Available: https://www.cso.com.au/article/666339/government-rewriting-cybersecurity-conversations-around-consumer-focus/. Last accessed 8 October 2019.

Brookes, C. (2015). *Cyber Security: Time for an integrated whole-of-nation approach in Australia. Australia*: The Centre for Defence and Strategic Studies (CDSS).

Browning, C.S. (2017). Security and migration: a conceptual exploration. In: Bourbeau, P. (ed.) *Handbook on Migration and Security*. United Kingdom: Edward Elgar Publishing. 39-59.

Burge, C. (2009). FIGHTING high tech crime. *Platypus Magazine* (103), 9.

Burgess, J.P. (2010). Introduction. In: Burgess, J.P *The Routledge Handbook of New Security Studies*. USA: Routledge. 1-5.

Burton, J. (2013). Cyber security: The strategic challenge and New Zealand's response. *New Zealand International Review*. 38 (3), 5-8.

Caballero-Anthony, M., Emmers, R. and Acharya, A. (eds.) (2006). *Non-Traditional Security In Asia.* England and USA*:* Ashgate.

Carr, M. (2016). Public–Private Partnerships in National Cyber-Security Strategies. *International Affairs*. 92 (1), 43-62.

CERT Australia. (2018). *Benefits of being a partner.* Available: https://www.cert.gov.au/jcsc/Benefits-of-being-a-partner. Last accessed 21 March 2019.

CERT Australia. (2018). *CERT Australia moving to ASD.* Available: https://webarchive.nla.gov.au/awa/20181009235245/https://www.cert.gov.au/news/cert-australia-moving-asd. Last accessed 8 October 2019.

CERT Australia. (2019a). *Sydney Joint Cyber Security Centre launch.* Available: https://webarchive.nla.gov.au/awa/20190305230224/https://www.cert.gov.au/news/sydney-

jcsc-launch. Last accessed 8 October 2019.

CERT Australia. (2019b). *Perth Joint Cyber Security Centre protecting West Australians.* Available: https://webarchive.nla.gov.au/awa/20190306014423/https://www.attorneygeneral.gov.au/Media/Pages/perth-joint-cyber-security-centre-protecting-west-australians-6-july-2018.aspx. Last accessed 8 October 2019.

Christensen, K.K. and Petersen, K.L. (2017). Public–private partnerships on cyber security: a practice of loyalty. *International Affairs*. 93 (6), 1435–1452.

Christou, C (2016). *Cyber security in the European Union: resilience and adaptability in governance policy*. London: Palgrave.

Christou, O. and Adamides, C. (2013). Energy securitization and desecuritization in the New Middle East. *Security Dialogue*. 44 (5-6), 507-522.

Cincotta, K. (2007). *Is Internet Banking Safe?.* Available: https://www.smh.com.au/technology/is-internet-banking-safe-20071213-gdrspm.html. Last accessed 25 August 2019.

Clinton, L. (2015). Best Practices for Operating Government-Industry Partnerships in Cyber Security. *Journal of Strategic Security*. 8 (4), 53-68.

Commonwealth of Australia. (2004). *House of Representatives Official Hansard*. 12. Canberra: Commonwealth of Australia.

Cornall, R. and Black, R. (2011). *Independent Review of the Intelligence Community*. Canberra: Commonwealth of Australia.

Crow, L. (2017). Gendered Bodies In Securitized Migration Regimes. In: Bourbeau, P. (ed.) *Handbook on Migration and Security*. United Kingdom: Edward Elgar Publishing. 39-59.

Culnane, C., Eldridge, M., Essex, A., Teague, V., and Yarom, Y. (2017). *iVote West Australia: Who Voted for You?.* Available: https://pursuit.unimelb.edu.au/articles/ivote-west-australia-who-voted-for-you. Last accessed 14 October 2019.

Cybercrime Act 2001. Available at https://www.legislation.gov.au/Details/C2004A00937. (Accessed 28 March 2019).

Defence Science and Technology Organisation. (2014). Future Cyber Security Landscape: A Perspective on the Future Canberra. Available at: https://www.dst.defence.gov.au/sites/default/files/publications/documents/Future-Cyber-Security-Landscape.pdf

Department of Defence under Payne, M. (2016). *Defence White Paper 2013.* Canberra: Australian Government Publishing Service.

Department of Defence. (1994). *Defending Australia: Defence White Paper.* Canberra: Australian Government Publishing Service.

Department of Defence. (2000). *Defence 2000: Our Future Defence Force.* Canberra: Australian Government Publishing Service.

Department of Defence. (2009). *Defending Australia in the Asia Pacific Century: Force 2030.* Canberra: Australian Government Publishing Service.

Department of Defence. (2013). *Defence White Paper 2013.* Canberra: Australian Government Publishing Service.

Department of Defence. (2016). *2016 Defence White Paper*. Canberra: Commonwealth of Australia.

Department of Defence. (2018). *New Cyber Security Centre to boost Australia's online resilience.* Available: https://www.minister.defence.gov.au/minister/marise-payne/media-releases/new-cyber-security-centre-boost-australias-online-resilience. Last accessed 21 March 2019.

Department of Defence. (2018). *New Cyber Security Centre to boost Australia's online resilience.* Available: https://www.minister.defence.gov.au/minister/marise-payne/media-releases/new-cyber-security-centre-boost-australias-online-resilience. Last accessed 21 March 2019.

Department of Home Affairs. (2019). Australia's 2020 Cyber Security Strategy: A call for views. Commonwealth of Australia. Available at: https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf. Last Accessed 8 October 2019.

Department of Human Services. (2019). *Cyber Security Strategy 2018-22.* Available: https://www.humanservices.gov.au/organisations/about-us/publications-and-resources/cyber-security-strategy-2018-22. Last accessed 8 October 2019.

Department of Prime Minister and Cabinet. (2013). *Strong and Secure: A Strategy for Australia's National Security.* Canberra: Commonwealth of Australia.

Department of Prime Minister and Cabinet. (2016). *Australia's Cyber Security Strategy.* Australia: Commonwealth of Australia.

Department of Prime Minister and Cabinet. (2017). Independent Intelligence Review. Canberra: Commonwealth of Australia.

Department of the Prime Minister and Cabinet. (2013). *Australian Cyber Security Centre*. [Press Release] 24 January 2013.

Department of the Prime Minister and Cabinet. (2014). *Cyber Security Review* [Press Release] 27 November 2014.

Department of the Prime Minister and Cabinet. (2017). *Independent Intelligence Review*. Canberra: Commonwealth of Australia.

Donaldson, D. (2019). *Cyber boss Alastair MacGibbon to return to private sector.* Available: https://www.themandarin.com.au/107983-cyber-boss-alastair-macgibbon-to-return-to-private-sector/. Last accessed 15 October 2019.

Dunn-Cavelty (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*. 15 (1), 105-122.

Dunn Cavelty M. (2014) *Introduction*. In: Cybersecurity in Switzerland. SpringerBriefs in Cybersecurity. Springer: Cham.

Dunn-Cavelty, M. and Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*. 2, 179-187.

Easton, S. (2019). *Infosec professionals join ACSC to improve national cyber resilience and, hopefully, policy.* Available: https://www.themandarin.com.au/103534-infosec-professionals-join-acsc-to-improve-national-cyber-resilience-and-hopefully-policy/. Last accessed 21 March 2019.

Enloe, C. (1983) Does Khaki Become You? The Militarisation of Women's Lives, South End: South End Press.

Finextra. (2004). *Phishing Scams Soar in 2004.* Available: https://www.finextra.com/newsarticle/12962/phishing-scams-soar-in-2004. Last accessed 25 August 2019.

Fitsanakis, J. (2012). Digital Sparta: Information Operations and Cyber-Warfare in Greece. In: Ventre, D *Cyber Conflict: Competing National Perspectives*. Great Britain and United States of America: ISTE Ltd. and Wiley and Sons

Fjäder, C.O. (2016). National Security in a Hyper-connected World. In: Masys, A.J *EditorExploring the Security Landscape: Non-Traditional Security Challenges*. New York: Springer. 31-59.

Flowers, A. and Zeadally, S. (2014). US Policy on Active Cyber Defense. *Homeland Security & Emergency Management*. 11 (2), 289–308.

Frewen, J. (2019). *Director-General's introduction.* Available: https://www.asd.gov.au/about/introduction. Last accessed 8 October 2019.

GAP Taskforce on Cyber Security. (2017). Protecting the New Frontier Report. Australia. Available at: https://www.globalaccesspartners.org/Cyber_Security_Taskforce_Report_GAP_Nov2017.pdf

Givens, A.D. and Busch, N.E. (2013). Realizing the promise of public-private partnerships in U.S. critical infrastructure protection. *International Journal of Critical Infrastructure Protection*. 6, 39-50.

Government of South Australia. (2019). *Cyber security strategy.* Available: https://dpc.sa.gov.au/responsibilities/ict-digital-cyber-security/cyber-security-strategy. Last accessed 8 October 2019.

Gray, P. (2004). *AU phishing scams to get worse.* Available: https://www.zdnet.com/article/au-phishing-scams-to-get-worse/. Last accessed 4 September 2019.

Hansen, L., Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*. 53 (4), 1155-1175.

Hare, F.B. (2009). Private Sector Contributions to National Cyber Security: A Preliminary Analysis. *Journal of Homeland Security and Emergency Management*. 6 Issue 1 (7), 1-20.

Harknett, R.J. and Stever, J.A. (2011). The New Policy World of Cybersecurity. *Public Administration Review*. 71 (3), 455-460.

Henderson, J. (2018). *New joint cyber security centre opens for business in Sydney.* Available: https://www.arnnet.com.au/article/634986/new-joint-cyber-security-centre-opens-business-sydney/. Last accessed 14 October 2019.

Jamieson, R., Land, L., Stephens, G. and Winchester, D. (Spring 2009). Identity crime: the need for an appropriate government strategy. *Forum on Public Policy: A Journal of the Oxford Round Table.* 1-33.

Jennings, P. and Feakin, T. (2013). SPECIAL REPORT: The emerging agenda for cybersecurity. Canberra: Australian Strategic Policy Institute's International Cyber Policy Centre. Available: https://www.files.ethz.ch/isn/167768/SR51_agenda_cybersecurity.pdf. Last accessed 14 October 2019.

Kaplan, F (2016). *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster.

Koski, C. (2015). Does a Partnership Need Partners? Assessing Partnerships for Critical Infrastructure Protection. *American Review of Public Administration*. 45 (3), 327-342.

Krone, T. (2005). Phishing: High Tech Crime Brief. *High Tech Crime Brief*, (9), 1-2.

Kuper, S. (2018). *Adelaide joins national cyber battle with launch of Joint Cyber Security Centre.* Available: https://www.defenceconnect.com.au/intel-cyber/3213-adelaide-joins-national-cyber-battle-with-launch-of-joint-cyber-security-centre. Last accessed 8 October 2019.

Leyden, J. (2004). *Trojan targets UK online bank accounts.* Available: https://www.theregister.co.uk/2004/11/12/banker_trojan/. Last accessed 2 September 2019.

Loiseau, H. and Lemay, L. (2012). Canada's Cyber Security Policy: a Tortuous Path Toward a Cyber Security Strategy . In: Ventre, D *Cyber Conflict: Competing National Perspectives*. Great Britain and United States of America: ISTE Ltd. and Wiley and Sons.

Lonsdale, D.J. (2016). Britain's Emerging Cyber-Strategy. *The RUSI Journal*. 161 (4), 52-62.

Luiijf, E., de Graaf, P. and Besseling, K. (2013). Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructure Protection*. 9 (1/2), 2-31.

MacGibbon, A. 2009. *Cyber Security: Threats and Responses in the Information Age. Australian Strategic Policy Institute.* https://www.aspi.org.au/news/release-aspi-special-report-cyber-security-threats-and-responses-information-age. Last accessed 13 October 2019.

Malone, E.F., and Malone, M.J. (2013). The "wicked problem" of cybersecurity policy:

analysis of United States and Canadian policy response. *Canadian Foreign Policy Journal*. 19 (2), 158–177.

McClure, D. (2018). *Calls for threat intel platform.* Available: https://www.innovationaus.com/2018/05/Calls-for-threat-intel-platform. Last accessed 21 March 2019.

McCombie, S. (2008). Trouble in Florida: the Genesis of Phishing attacks on Australian Banks. Australian Digital Forensics Conference.

McCombie, S. (2011). 'Phishing the Longline: Transnational Cybercrime from Eastern Europe to Australia', Doctor of Philosophy, Deakin University.

McCombie, S. and Pieprzyk, J. (2010). Winning the Phishing War: A Strategy for Australia. *2010 Second Cybercrime and Trustworthy Computing Workshop*. IEEE: Computer Society, 79-86.

McDonald, M. (2008). Securitization and the Construction of Security. *European Journal of International Relations*. 14 (4), 563-587.

McDonald, M. (2013). Constructivism. In: Williams, P.D (ed.) *Security Studies: An Introduction*. New York: Routledge. 59-73.

McKenzie, S. (2006). 'Partnership Policing of Electronic Crime: An Evaluation of Public and Private Police Investigative Relationships', Doctor of Philosophy, University of Melbourne.

Moffette, D. and Vadasaria, S. (2016). Uninhibited violence: race and the securitization of immigration. *Critical Studies on Security*. 4 (3), 291-305.

Morag, N. (2011). Security Policies: Critical Infrastructure Protection, Public–Private Partnerships, and Aviation, Chapter 7: Maritime, and Surface-Transport Security. In: *Comparative homeland security: global lessons* . United States: John Wiley & Sons. 261-289.

Mutimer, D. (2010). Critical Security Studies. In: Cavelty, M.D. and Mauer, V. *The Routledge Handbook of Security Studies*. New York and London: Routledge. 45-55.

Nakashima, E. (2014). *U.S. notified 3,000 companies in 2013 about cyberattacks.* Available: https://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html. Last accessed 8 October 2019.

Nikitakos, N. and Mavropoulos, P. (2014). Cyberspace as a State's Element of Power. In: Carayannis, E.G., Campbell, D.F.J., and Efthymiopoulos, M.P *Cyber-Development, Cyber-Democracy and Cyber-Defense Challenges, Opportunities and Implications for Theory, Policy and Practice*. New York: Springer. 259-279.

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology*. 7 (2), 61-73.

Office of the Cyber Security Special Advisor. (2016). Review of the Events Surrounding the 2016 eCensus: Improving institutional cyber security culture and practices across the Australian government. Commonwealth of Australia.

Parliament of Australia. (2006a). *Australian Crime Commission Committee Report: Government Response: Senate Hansard*, Available at: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansards%2F2006-02-09%2F0128%22

Parliament of Australia. (2006b) Senate Standing Committee on Legal and Constitutional Affairs: Supplementary Budget Estimate 2006-2007: Hansard. Available at:

https://www.aph.gov.au/~/media/Estimates/Live/legcon_ctte/estimates/sup_0607/agd/qon_173.ashx. Last accessed 13 October 2019.

Parliament of Australia. (2007). Senate Standing Committee on Legal and Constitutional Affairs: AFP of 2007 Hansard: Canberra. Available at: https://webarchive.nla.gov.au/awa/20070923145317/http://wopared.aph.gov.au/Senate/committee/legcon_ctte/estimates/add_0607/ag/qon_136.pdf. Last accessed 13 October 2019.

Parliament of Australia. (2010). Hackers, fraudsters and botnets tackling the problem of cybercrime: the report of the inquiry into cybercrime. House of Representatives, Standing Committee on Communications: Australia. Available at: https://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=coms/cybercrime/report.htm. Last accessed: 13 October 2019.

Parliament of Australia. (2018). Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Bill 2018 [provisions]. Canberra: Commonwealth of Australia. Available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Affairs_Defence_and_Trade/ASD/Report/c01

Parliament of Australia. (2019). *Australia's National Security: a Defence Update 2003, 2005 and 2007.* Available: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1516/DefendAust/NationalSecurity#_ftn26. Last accessed 13 October 2019.

Parliament of Western Australia (2018) Extract from Hansard ASSEMBLY: p6680b-6681a. Tuesday, 9 October 2018 Available at: https://www.parliament.wa.gov.au/Hansard/hansard.nsf/0/bd4e2e781afc6d814825838a000d287b/$FILE/A40%20S1%2020181009%20p6680b-6681a.pdf.

Pearce, R. (2017). *Government launches Melbourne Joint Cyber Security Centre.* Available: https://www.computerworld.com.au/article/628466/government-launches-melbourne-joint-cyber-security-centre/. Last accessed 21 March 2019.

Pearce, R. (2018). *From signals to cyber: Inside the transformation of the Australian Signals Directorate.* Available: https://www.computerworld.com.au/article/648710/from-signals-cyber-inside-transformation-australian-signals-directorate/. Last accessed 8 October 2019.

Pearce, R. (2019). *Budget 2019-20: Government to create cyber 'sprint teams'.* Available: https://www.computerworld.com.au/article/659578/budget-2019-20-government-create-cyber-sprint-teams/. Last accessed 8 October 2019.

Platypus. (2009). FIGHTING high tech crime. *Platypus Magazine*(103), 7-8.

Portillo-Castro, H. (2019). *Cyber policy: Budget Review 2018–19 Index.* Available: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/BudgetReview201819/CyberPolicy#_ftn13. Last accessed 8 October 2019.

Reichert, C. (2019). *Australian Budget 2019: Whole-of-government cyber uplift to create 'cyber sprint teams'.* Available: https://www.zdnet.com/article/australian-budget-2019-whole-of-government-cyber-uplift-to-create-cyber-sprint-teams/. Last accessed 8 October 2019.

Reveron, D.S. (ed.) (2012). *Cyberspace and National Security: Threats, Opportunities and Power, in a Virtual World*. United States of America: Georgetown University Press.

Riley, J. (2019). *ACSC shutters 2019 conference.* Available: https://www.innovationaus.com/2019/01/ACSC-shutters-2019-conference. Last accessed 8 October 2019.

Ruohonen, J., Hyrynsalmi, S. and Leppänen, V. (2106). An outlook on the institutional evolution of the European Union cyber security apparatus. *Government Information Quarterly*. 33 (1), 746–756.

Rusch, J. (2005). The compleat cyber-angler: a guide to phishing. *Computer Fraud & Security*. 1 (1), 4-6.

Sanger, D.E. (2018). *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*. Australia and the United Kingdom: Scribe.

Shakarian, P. Shakarian, J. and Andrew Ruef. (2013) *Introduction to Cyber-Warfare: A Multidisciplinary Approach.* Amsterdam and Boston: Syngress.

Sigston, D. (2017). *Joint Cyber Security Centre opens in Brisbane.* Available: https://www.couriermail.com.au/news/queensland/crime-and-justice/joint-cyber-security-centre-opens-in-brisbane/news-story/51eb5b6c42f683bc1dfad73c69dda7be?nk=29a2e8c910c1a7091b0bebd5ce6a4c76-155315793. Last accessed 21 March 2019.

Singer, P.W. and Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. United States of America: Oxford University Press.

Slocombe, G. (2013). Cyber security: A vital part of national security. *Asia-Pacific Defence Reporter*. 39 (2), 31-34.

Smith, F. and Ingram, G. (2017). Organising cyber security in Australia and beyond. *Australian Journal of International Affairs*. 71 (6), 642-660.

The Centre for International Governance Innovation [CIGI]. (2018). *Governing Cyber*

Security in Canada, Australia and the United States. Canada: Carrol Bonnett.

Spencer, L. (2017). *Govt boosts industry collaboration with new Joint Cyber Security Centre.* Available: https://www.arnnet.com.au/article/628453/govt-boosts-industry-collaboration-new-joint-cyber-security-centre/. Last accessed 8 October 2019.

Stilgherrian. (2019). *ACSC dumps annual conference, partners with AISA for cyber events.* Available: https://www.zdnet.com/article/acsc-dumps-annual-conference-partners-with-aisa-for-cyber-events/. Last accessed 8 October 2019

Sydney Morning Herald (SMH). (2003). *Police launch hi-tech crime centre.* Available: https://www.smh.com.au/national/police-launch-hi-tech-crime-centre-20030702-gdh143.html. Last accessed 3 September 2019.

van Niekerk, B. and Maharaj, M. (2012). A South African Perspective on Information Warfare and Cyber Warfare. In: Ventre, D *Cyber Conflict: Competing National Perspectives*. Great Britain and United States of America: ISTE Ltd. and Wiley and Sons.

Ventre, D. (ed.) (2012). *Cyber Conflict: Competing National Perspectives*. Britain and United States of America: ISTE Ltd. and Wiley and Sons.

Wæver, O. (1995). 'Securitization and Desecuritization', in Ronnie D. Lipschutz (ed.) *On Security*, New York: Columbia University Press, 46–86.

Warren, M. and Leitch, S. (2018). Australian cyber security policy through a European lens. *ECCWS 2018: Proceedings of the 17th European Conference on Cyber Warfare and Security*. Academic Conferences International Limited, Reading, Eng, 489-495.

Warren, M. & Leitch, S. (2011). *Australian National Critical Infrastructure Protection: A Case Study*, Academic Conferences International Limited, Reading.

Watson, S.D (2009). *The Securitisation of humanitarian migration: Digging moats and sinking boats*. London: Routledge.

Watson, S.D. (2012). Framing the Copenhagen School: Integrating the Literature on Threat Construction. *Millennium: Journal of International Studies*. 40 (2), 279-301.

Williams, D. (2001). Attorney-General's Department's *E-Security Initiative- Protecting the National Information Infrastructure*. [Press Release].

Williams, D. (2006). Attorney-General's Department. *E-Security Initiative- Protecting the National Information Infrastructure*. [Press Release].

Yin, R.K. (2009). *Case Study Research: Design and Methods*. 4th ed. United States of America: Sage Publications.

Yin, R.K. (2012). *Applications of Case Study Research*. United States of America: Sage Publications.

Young, K. (2004). *Phishing Phobia.* Available: https://www.theguardian.com/technology/2004/nov/18/money.newmedia. Last accessed 25 August 2019.

Zimmermann, H. (2017). Exporting Security: Success and Failure in the Securitization and Desecuritization of Foreign Military Interventions. *Journal of Intervention and Statebuilding*. 11 (2), 225-244.