FLINDERS UNIVERSITY

FACULTY OF SOCIAL AND BEHAVIOURAL SCIENCES

SCHOOL OF INTERNATIONAL STUDIES

DEPARTMENT OF INTERNATIONAL RELATIONS

STATE OF VULNERABILITY:
AUSTRALIA-US CYBER MATURITY

MATTHEW HOLDING

ADELAIDE, 14 MAY 2017

This thesis is submitted in partial fulfilment of the requirements of the degree of Masters of Arts (International Relations)

DECLARATION

I certify that this thesis does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any university, and that to the best of my knowledge and belief it does not contain any material previously published or written by another person, except where due reference is made in the text.

Name: ………………………………

Date: ………………………………..

Table of Contents

SYNOPSIS

This thesis examines the efforts made by Australia and the United States to improve their own cyber governance and to cooperate with each other on cybersecurity. Effective cyber governance is measured by the strength of a state's cyber maturity which is demonstrated by the presence and implementation of effective cyber-related structures, policies, legislation and organisations. With the use of a theoretical framework this thesis examines both states cyber maturity through four specific categories. These categories are: (1) accurate threat analysis; (2) coordinated institutional structure; (3) coherent cyber policy, and (4) establishment of cyber defence responsibility. Analysing these states cyber maturity and their cooperation through this framework allows for a deeper understanding of contemporary trends of cyber governance as well as the threats and challenges which national government's face. This thesis concludes that both states have developed cyber governance which will largely result in strong cyber maturity. In a global security climate where cyberspace is becoming more vulnerable and compromised, both states made strong efforts to develop cyber governance which best positions them to defend against the future of cyber threats. Furthermore, this thesis finds that both states have made efforts to strengthen their historical alliance by committing to cyber cooperation. Through institutional alliance collaboration, Australia and the US have focused on deepening their cyber engagement to advance their respective economic and security interests.

ACKNOWLEDGEMENTS

I would like to extend my thanks to the following: my supervisor, Dr. Maryanne Kelton, for her endless guidance, wisdom and encouragement throughout the year; Stefanie Van Gerven, for her tireless support, motivation and care from the beginning to end of writing this thesis; my parents, for supporting me throughout my studies, Prof. Anthony Langlois; for always being a source of encouragement, advice and insight throughout my Master's degree; my fellow students and staff at the Flinders University School of History and International Relations; and finally my friends for always being a source of enthusiasm.

LIST OF ACRONYMS

ACSC – Australian Cyber Security Centre

AFP – Australian Federal Police

ANZUS – The Australia, New Zealand, United States Treaty

ASD – Australian Signals Directorate

ASIO – Australian Security Intelligence Organisation

ASPI – Australian Strategic Policy Institute

ASIS – Australian Secret Intelligence Service

AUSMIN - Australia-United States Ministerial Consultations

BOM – Bureau of Meteorology

CERT – Computer Emergency Response Team

CIA – Central Intelligence Agency

CIIT – Cyber Threat Intelligence Integration Center

CIP – Critical Infrastructure Protection

CS&C – Office of Cyber Security and Communications

CSC – Homeland Security Council and Cybersecurity Coordinator

CNAP – Cybersecurity National Action Plan

CSIS – Center for Strategic and International Studies

DDOS – Distributed Denial-Of-Service Attacks

DHS – Department of Homeland Security

DOD – US Department of Defense

DOJ – Department of Justice

DOS – Department of State

FBI – Federal Bureau of Investigation

IC – US Intelligence Community

IS – Islamic State

ICI-IPC – Information and Communication's Infrastructure Interagency Policy Committee

NCTP – 2012 Australian National Counter-Terrorism Plan

NICCS – National Initiative for Cybersecurity Careers and Studies

NSA – National Security Agency

US – United States of America

US-CERT – United States Computer Readiness Team

USCYBERCOM – US Cyber Command

LIST OF FIGURES

INTRODUCTION

In a global security climate, characterized by anxiety regarding the rapid growth of technology and cyberspace, the importance of national governments strengthening their cybersecurity capabilities cannot be understated.[1] A growing risk of cyber threats from both state and non-state actors have forced contemporary western governments to prioritize cybersecurity amongst the highest of national security concerns.[2] Current cyber threats, which can be considered the biggest challenges for states, include: the risk of cyberattacks on critical infrastructure by state and non-state actors; the use of the internet as a recruitment and propaganda tool by non-state terrorist groups; cybercrime as well as state-based surveillance; and theft of intellectual property and sensitive information.[3] A growing threat is the risk of soft power cyberattacks whereby both state and non-state actors disseminate sensitive information, often obtained through hacking.[4] These types of cyber campaigns are intended to undermine democracy and confidence for the target state's political institutions, potentially with the end goal of influencing the outcome of an election to serve the interests of the perpetrator.[5] Contemporarily, the objectives and motivations of threat actors who commit cyberattacks broadly include political, economic and socio-cultural motivations.[6]

Cyber threat prioritization between state and non-state actor threats is one of the biggest concerns for national governments. William Marmon assesses the threat from state actors as higher than non-state actors due to their greater technical capabilities to cause damage to

[1] G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security*, May 2016, pp. 3-9.

[2] L. Gribbon, V. Horvath, K. Robertson, N. Robinson, 'Cyber-security Threat Characterisation: A Rapid Comparative Analysis', *RAND Corporation*, 2013, p. viii.

[3] *Ibid*, pp. viii-x.

[4] M. Aaolta, M. Mattiisen, Election Hacking in Democracies: The Example of The U.S. 2016 Elections, *The Finnish Institute of International Affairs*, FIIA Briefing Paper 204, October 2016, pp. 2-4, 6-7.

[5] B. Buchanan, M. Sulmeyer, Hacking Chads: The Motivations, Threats, and Effects of Electoral Insecurity, *Belfer Center for Science and International Affairs*, October 2016, pp. 3-15.

[6] L. Gribbon, V. Horvath, K. Robertson, N. Robinson, 'Cyber-security Threat Characterisation: A Rapid Comparative Analysis', *RAND Corporation*, 2013, pp. 5-6.

critical infrastructure.[7] Part of the high threat evaluation for state-based cyberattacks is the high potential for tension between adversarial great powers such as the United States, China, Russia, and Iran being played out in cyberspace. This tension has led to anxiety regarding the looming threat of cyber conflict.[8] Besides the nightmare cyber scenario of a disastrous cyberattack on critical infrastructure, state-based cyber threats have created increased tension between states due to the heightened threat of state-based cyberespionage, and cyber theft of intellectual property and sensitive national security information.[9] The cyber threat landscape has left governments extremely vulnerable; this is due to a paradigm shift in which experts believe that previous approaches to cybersecurity are outdated. Previous approaches were focused on building strong networks to defend against cyber threats. Christian Leuprecht now believes that these networks are already compromised and states need to focus cyber policy on defending against threats in an already breached environment.[10] A common mentality within cyber governance regards cyber defence infrastructure as a wall-based defence system, this mentality risks creating a blind spot to some of the most considerable forces preventing progress in cyber governance. It is the Leuprecht's belief that in reality, a great deal of cyber defence infrastructure adds little to real defence but only creates the illusion that strong cyber defence is in place.[11] The vulnerabilities of cyberspace have extended into critical domains, which in turn have created a strategic challenge for the security of the modern state, state sovereignty and international relations.[12] These heightened threats have contributed to the

[7] W. Marmon, 'Main cyber threats now coming from governments as "state actors"', *The European Institute*, November 2011, https://www.europeaninstitute.org/index.php/136-european-affairs/ea-november-2011/1464-main-cyber-threats-now-coming-from-governments-as-state-actors, accessed 10 March 2017.

[8] K. Breene, 'Who are the cyberwar superpowers?', *World Economic Forum*, 4 May 2016, https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/, accessed 10 March 2017.

[9] A.S. Cevallos, S.W. Harold, M.C. Libicki, 'Getting to yes with China in Cyberspace', *Rand Corporation,* 2016, pp. 6-8.

[10] C. Leuprecht, D.B. Skillicorn, V.E. Tait, 'Beyond the Castle Model of cyber-risk and cyber-security', *Government Information Quarterly*, Elsevier, 2016, pp. 1-3.

[11] *Ibid.*

[12] Z. Hawkins, L. Nevill, 'Deterrence in cyberspace: Different domain, different rules', *Australian Strategic Policy Institute*, July 2016, p. 5.

prioritization of cybersecurity as a key focus of their national security and foreign policy agenda as well as the rapid growth of state's militarization of their cyber defences.[13]

The rapid growth of technology in an interconnected world has created a new cyber landscape whereby cyberspace is being weaponized for offensive and often malicious capabilities. Hence, state actors have been forced to place cybersecurity at the forefront of their national security agenda and create cyber policy, which strengthens their resilience against these threats.[14] Protecting vulnerable critical infrastructure, sensitive information, cooperating with allies to promote cyber norms as well as deterring threats, which aim to de-stabilize national security and undermine democratic institutions, will be key policy priorities for governments for the foreseeable future.[15]

As historically strong allies based on shared strategic interests and values, Australia and the US are committed to cooperating with one another on building cyber-capacity.[16] In a rapidly growing cyber landscape, it is inevitable that Australia and the US would expand their strategic relationship to enable strong cyber cooperation.[17] Through institutional alliance collaboration such as ANZUS,[18] The US-Australia Cyber Dialogue[19] and the UKUSA Treaty (otherwise known as Five Eyes),[20] both states have committed to cyber engagement to advance their respective security and economic interests. Furthermore, both states are

[13] I. Wallace, 'The Military Role in National Cybersecurity Governance', *Brookings Institution*, 16 December 2013, https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/, accessed 23 September 2016.

[14] A. Macgibbon, 'Cyber security: threats and responses in the information age', *Australian Strategic Policy Institute*, Issue. 26, December 2009, pp. 6-12.

[15] Z. Hawkins, L. Nevill, 'Deterrence in cyberspace: Different domain, different rules', *Australian Strategic Policy Institute*, July 2016, pp. 5-8.

[16] T. Feakin, 'The US-Australia Cyber Dialogue: prioritising cyber between strategic partners', *Australian Strategic Policy Institute*, 25 October 2016, https://www.aspistrategist.org.au/prioritising-cyber-strategic-partners-us-australia-cyber-dialogue/, accessed 18 January 2017.

[17] D. Nichola, 'Expanding Alliance: ANZUS Cooperation and Asia-Pacific security', *Australian Strategic Policy Institute*, December 2014, pp. 20-21.

[18] Ibid.

[19] T. Feakin, 'The US-Australia Cyber Dialogue: prioritising cyber between strategic partners', *Australian Strategic Policy Institute*, 25 October 2016, https://www.aspistrategist.org.au/prioritising-cyber-strategic-partners-us-australia-cyber-dialogue/, accessed 18 January 2017.

[20] S. Cushing, A. Moens, A.W. Dowd, 'Cybersecurity Challenges for Canada and the United States', *Fraser Institute*, March 2015, pp. 20-23.

working together to promote cyber norms of a free and open internet alongside the deterrence of malicious cyber threats.[21] More specifically, cyber cooperation will be facilitated through expanded information sharing, coordinated technological investment[22] and the commitment to fight cybercrime.[23] In an effort to collaborate with multiple sectors on cybersecurity, both states have agreed to engage in cybersecurity orientated public-private partnerships in the Asia-Pacific.[24]

Using a framework constructed from contemporary theoretical cybersecurity perspectives, this thesis asks how advanced is the cyber maturity of both Australia and the US in response to the threat of malicious cyber threats from both state and non-state actors. Furthermore, this thesis asks to what extent can these states cooperate in the effort to defend against these types of threats. As such it investigates whether these states have achieved a sufficient level of cyber maturity. Here, the term 'cyber maturity' can be used as a term to assess the various facets of state cyber capabilities. Cyber maturity can be understood as a demonstration of the presence, effective implementation and operation of cyber-related structures, policies, legislation and organisations.[25] As there is currently a dearth of academic literature on the topic of Australia-US cyber cooperation, it is the goal of this thesis to pursue a niche in this new and largely unexplored field of academic research within international relations, intelligence and cybersecurity studies. This thesis analyses the growth of cyber governance within Australia and the US in the period between the September 11, 2001 attacks and the 2016, November 8th election of Donald J. Trump.

[21] Z. Hawkins, 'The US-Australia Cyber Dialogue: cooperation in the Asia-Pacific', *Australian Strategic Policy Institute*, 1 November 2016, https://www.aspistrategist.org.au/us-australia-cyber-dialogue-cooperation-asia-pacific/, accessed 21 January 2017.

[22] D. Nichola, 'Expanding Alliance: ANZUS Cooperation and Asia-Pacific security', *Australian Strategic Policy Institute*, December 2014, pp. 20-21.

[23] Z. Hawkins, L. Nevill, 'The US-Australia Cyber Dialogue: fighting cybercrime in the Asia-Pacific', *Australian Strategic Policy Institute*, 4 November 2016, https://www.aspistrategist.org.au/us-australia-cyber-dialogue-fighting-cybercrime-asia-pacific/, accessed 23 January 2017.

[24] *Ibid.*

[25] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2016', *Australian Strategic Policy Institute*, 2016, p.5.

The thesis begins in Chapter One by establishing a theoretical framework which will be used in later chapters to assess Australia-US cyber maturity and their cyber relationship. The framework is used to analyse the cyber maturity of a state's cybersecurity governance. The framework of analysis comprises four categories essential for cyber maturity. The categories are accurate threat analysis, coordinated institutional structure, coherent cyber policy as well as establishment of cyber defence responsibility. The analysis used in the framework is derived from the works of key theorists with expertise in contemporary cyber policy[26] These experts are associated with a number of influential Australian and international foreign policy and cybersecurity think tanks, academic institutions and government institutions. Given that cybersecurity is a diverse and broad field, a deeper scope of analysis is necessary to measure cyber maturity through these categories of focus, which concentrate on precise areas of cybersecurity. Evidence of cyber maturity in each category suggests a strong culture of defence against cyber threats.

The first category of analysis is accurate threat analysis. A state's ability to process accurate threat analysis is dependent on three factors, which will result in cyber maturity. These

[26] L. Gribbon, V. Horvath, K. Robertson, N. Robinson, 'Cyber-security Threat Characterisation: A Rapid Comparative Analysis', RAND Corporation, 2013; G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security*, May 2016; Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2015', *Australian Strategic Policy Institute*, 2015; B. Akhgar, F. Bosco, A. Staniforth, Cyber Crime and Cyber Terrorism Investigator's Handbook, Syngress, 2014; A. MacGibbon, 'Cyber Security: Threats and Responses in the Information Age', *Australian Strategic Policy Institute*, December 2009, Issue 26; T. Feakin, P. Jennings, 'The Emerging Agenda for Cybersecurity', *Australian Strategic Policy Institute*, July 2013; P.W. Singer, 'The Cyber Terror Boogeyman', *Brookings Institution*,, 1 November 2012, https://www.brookings.edu/articles/the-cyber-terror-bogeyman/, accessed 10 September 2016; G. Weimann, 'Cyberterrorism: How Real is The Threat?', *United States Institute of Peace*, December 2004, https://www.usip.org/sites/default/files/sr119.pdf, accessed 4 September 2016; K.M. Finklea, 'The Interplay of Borders, Turf, Cyberspace and Jurisdiction: Issues Confronting U.S. Law Enforcement', *Congressional Research Service*, 17 January 2013, pp. 20-24; K. Von Knop, 'Institutionalization of a Web-Focused, Multinational Counter-Terror Campaign', Responses to Cyber Terrorism', *Centre of Excellence Defence Against Terrorism*, 2008; I. Wallace, 'The Military Role in National Cybersecurity Governance', *Brookings Institution*, 16 December 2013, https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/, accessed 23 September 2016; A. Ariely, 'Adaptive Responses to Cyberterrorism', Cyberterrorism: Understanding, Assessment, and Response, Springer Publishing, 2014, pp. 180-18; Z. Hawkins, L. Nevill, 'National cyber budgets', same, same but different', *Australian Strategic Policy Institute*, 16 June 2016, https://www.aspistrategist.org.au/national-cyber-budgets-different/, accessed 20 September 2016; A. Dupont, 'Cybersphere is the Globe's New Battlefront', *The Lowy Institute*, 26 April 2016, http://www.lowyinstitute.org/publications/cybersphere-globes-new-battlefront, accessed 24 September 2016.

factors include the ability to accurately assess the nature of the cyber threat itself, the nature of risk associated with the threat and finally the nature of the actor responsible the threat. .[27] Second, a component necessary for strong cyber maturity is a coordinated institutional cyber structure; this refers to how states develop an institutional cyber structure which informs cyber maturity. The thesis argues third, that well-thought out cyber policy informs a state's cyber maturity. A state's ability to develop coherent cyber policy, which will result in cyber maturity, is dependent on a number of consistent components. Finally the thesis argues that, a state's ability to develop cyber defence responsibility is imperative to attain strong cyber maturity. [28] Cyber defence responsibility can understood as the ability for agencies responsible for cybersecurity to cooperate and balance responsibility with one another.

With the use of the framework, Chapter Two provides analysis of Australia's current cybersecurity infrastructure and capabilities and assesses the strength of its cyber maturity, it also analyses Australia's cyber challenges. Chapter Three then seeks to apply the same analysis to current state of US cybersecurity governance. Finally, Chapter Four analyses how both states are currently cooperating on cybersecurity and provides recommendations as to why Australia and the US should deepen their cyber cooperation to both strengthen their strategic alliance and cyber maturity.

[27] L. Gribbon, V. Horvath, K. Robertson, N. Robinson, 'Cyber-security Threat Characterisation: A Rapid Comparative Analysis', RAND Corporation, 2013, pp. viii-x.

[28] B. Akhgar, F. Bosco, A. Staniforth, Cyber Crime and Cyber Terrorism Investigator's Handbook, Syngress, pp. 40-41.

CHAPTER ONE:
The Achievement of Cyber Maturity

INTRODUCTION

Given anxiety within society regarding the prevalence of cyber threats, it is fundamental to examine the contemporary literature which examines these threats.[29] This chapter will examine the cyberterrorism literature in order to create a framework, which will be used in later chapters as a systematic method to analyse Australia and US cyber maturity. It will include an analysis of the parameters of cyber threats in order to clearly understand the wide-ranging challenges that international governments face.

The cyber maturity categories which will be examined include: accurate threat analysis; coordinated institutional structure of cyber governance; coherent cyber policy; and establishment of cyber defence responsibility. Attaining a balance of strong cyber maturity in all of these categories is vital to creating a strong culture of defence against cyber threats.[30] It can be argued that the three most important factors of cyber maturity are: healthy cooperation between cyber departments as well as between international allies and with the private sector; promotion of cyber education; and critical infrastructure protection (CIP).[31]

THE PARAMETERS OF CYBER THREATS AND CYBERTERRORISM

The thesis uses the following definition of cyberterrorism in its analysis: the intentional use of computers, networks and public internet to cause destruction and harm for personal objectives.[32] Cyberattacks are often carried out with the intention to cause either: harm, fear or hysteria for furthering the individual or group's social, ideological, religious or political

[29] G. Weimann, 'Cyberterrorism: How Real is The Threat?', *United States Institute of Peace*, December 2004, https://www.usip.org/sites/default/files/sr119.pdf, accessed 4 September 2016, pp. 2-3.

[30] 'Cyber Maturity in the Asia-Pacific Region 2015', *Australian Strategic Policy Institute*, 2015, pp. 5-8.

[31] G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security*, May 2016, pp. 20-23.

[32] J. Matusitz, 'Cyberterrorism: How Can American Foreign Policy Be Strengthened In The Information Age?', *American Foreign Policy Interests*, Vol. 27, No. 2, April 2005, p. 137.

goals.[33] For the purpose of widening the scope of the threat of cyberterrorism, this study uses this definition as to understand the broad range of threats associated with contemporary security challenges in the cyber sphere. This is to allow the inclusion of state-based cyber threats, which this thesis argues, are the primary threat that national government's face.. Furthermore, the study applies this definition of cyberterrorism as it allows for the understanding of the use of cyberspace as a radicalization and recruitment tool, fundraising and networking space, propaganda device and for the purpose of non-cyber-attack planning and coordination by terrorist organizations.[34]

As the following section now reveals, consultation of the literature suggests four categories of cyber governance essential for cyber maturity. These categories are: 1. accurate threat analysis; 2. coordinated institutional structure; 3. coherent cyber policy; 4. establishment of cyber defence responsibility.

ACCURATE THREAT ANALYSIS

The first part in the process of establishing cyber maturity is accurate threat analysis. A state's ability to accurately analyse cyber threats is dependent on three factors. First: a state must identify the nature of the threat. This means detecting what specific technical types of cyber threats and attacks national government's face. Second: a state must identify the danger of the threat. This refers to the risk of damage and judgement of vulnerability that an actor can cause to its target.[35] Third: a state must identify the nature of the actor responsible for the cyber threat. This refers to identifying whether the actor is a state or non-state actor and their capabilities.

[33] J.W. Rollins, C.A. Theohary, 'Cyberwarfare and Cyberterrorism: In Brief', *Congressional Research Service*, 17 March 2015, https://fas.org/sgp/crs/natsec/R43955.pdf, accessed 1 September 2016, p. 1.

[34] G. Weimann, 'Cyberterrorism: The Sum of All Fears?', *Studies in Conflict & Terrorism*, Vol. 28, 2005, pp. 130-140.

[35] L. Gribbon, V. Horvath, K. Robertson, N. Robinson, 'Cyber-security Threat Characterisation: A Rapid Comparative Analysis', *RAND Corporation*, 2013, pp. ix-x.

In terms of analysing the nature of the threat and the risk associated, The Monterey Group for the Special Oversight Panel on Terrorism Committee of the US House of Representatives adopts a three-level categorization to evaluate cyberterror attacks.[36] This categorization is as follows:

> **Simple-Unstructured**: The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command or control, or learning capability.[37]
>
> **Advanced-Structured:** The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.[38]
>
> **Complex-Coordinated:** The capability for a coordinated attack causing mass-disruption against integrated, heterogeneous defences (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organization learning capability.[39]

Categorizations like these are useful in analysing the varying threat levels of different cyberterrorist actors and organizations.

At present, research shows state-based cyber threats are prioritized as a greater risk than non-state actors. Nation-states have higher technological capabilities to inflict damage on national

[36] Denning, D. E., “Cyberterrorism,” Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, 23 March, 2000.
[37] *Ibid.*
[38] *Ibid.*
[39] *Ibid.*

critical infrastructure and conduct cyber espionage.[40]To compare cyber threat awareness, Robinson, Gribbon, Horvath and Robertson of RAND Corporation have constructed a comparative global analysis of cybersecurity threat characterization for European states, Canada and the US. Canada, the Netherlands and the UK who have prioritized the migration of foreign-state espionage to the cyber territory as a threat of high concern. Some governments focus on particular threat instances, for example, Canada placed a high level of concern on the risk of a cyberattack of national infrastructure occurring during a national disaster.[41] The study also identifies both rogue states and peer competitor states as being threats whose goals can be categorized as both deterring, defeating and raising the cost of a state's involvement in a regional dispute as well as deterring or deferring a country in major confrontation, espionage or economic advantage.[42]

These findings indicate that generally the states analysed recognise state-based actors as being of the highest concern.[43] The study suggests that states are largely responsive to events and there has been a shift from focusing on transnational, terrorist threat actors to reframing cybersecurity in terms of defence and offensive capabilities against cybercriminals, state actors and their terrorist proxies.[44] Based on their findings some of the cyber threat areas which are of most concern to these governments, include:

- Distributed Denial-Of-Service (DDOS) attacks.[45]
- China's digital espionage capabilities.[46]
- Cybercrime: Organised criminal's attacks against business intellectual property.[47]

[40] *Ibid*, pp. viii-ix.
[41] *Ibid.*
[42] *Ibid.*
[43] *Ibid*, p. ix
[44] *Ibid.*
[45] *Ibid.* A Distribution Denial-Of-Service attack where a perpetrator attempts to make an online service unavailable by flooding of the system by overwhelming it with traffic from multiple services.
[46] *Ibid.*

- Cyberespionage: Targeting of financial systems and government protectively marked information.[48]

Furthermore, this study found that there is little evidence that these states have processes in place to forecast what future threat actors may appear on the cyber scene. It also suggests that states would be wise to distinguish between risk and threat, threats being types of actors that might act strategically and risks being judgements about vulnerabilities and impact. By doing so, governments stand a better change of safeguarding themselves against and responding to cyber threats.[49]

Other common threats included were those from individuals whose goals were focused on mayhem and vandalism. These include coordinated sub- or pan-national groups or networks (terrorists, hacktivists, and organised crime) whose goals were focused on gaining money or power as well as gaining support. Their goal is to create fear and disruption through protest with the goal of overthrowing governments.[50] Because non-state cyberterrorism is commonly discussed in public discourse it has heightened anxiety regarding this threat, however the main focus of accurate threat analysis is on state-based threats for states with strong cyber maturity.

Non-state cyberterrorism can be assessed as a secondary focus compared to state-based threats because public anxiety regarding the threat of cyberterrorism is can be considered largely overblown; Singer believes society has let our fear of threats obscure how terrorists really use the internet.[51] He believes that in reality, there have been very few instances of cyberterrorism, which has caused great damage or suffering and that by analysing how terror

[47] *Ibid.*
[48] *Ibid.*
[49] *Ibid*, pp. ix-x.
[50] *Ibid*, pp. 5-6.
[51] P.W. Singer, 'The Cyber Terror Boogeyman', *Brookings Institution*, 1 November 2012, https://www.brookings.edu/articles/the-cyber-terror-bogeyman/, accessed 10 September 2016.

groups actually use the internet, rather than obsessing over doomsday scenarios, we can properly prioritize and focus our efforts.[52]

Inaccurate risk evaluation can be viewed as one of the biggest challenges for threat analysis. In regards to cyberterrorism, contemporary society conflates its fears regarding cyberterrorism with the actual state of affairs regarding terrorism. For instance, Singer believes that very few cyberterrorists have the means and capabilities to pull off attacks which are at the forefront of society's cyber angst, and include large-scale attacks on electrical grids and hydroelectric generators.[53] Singer states that despite many terror groups not having the capabilities to execute large-scale attacks, this does not mean that they are not interested in using cyberspace to cause violence. More focus should be on the way in which terrorists use the internet, focusing more so on the internet as a tool for propaganda, recruitment, collecting and spreading of information, which he believes has a greater threat risk to human safety than large scale cyberattacks on information systems.[54]

Another major challenge for accurate threat analysis is the ability for states to precisely calibrate and assess the risk of threats in public discourse. Understanding the threat level attached with cyber threats and cyberterrorism is critical in defending against cyberattacks and raising public awareness. On the one hand, cyberterrorism takes a high psychological toll on society.[55] Weimann believes that this fear has been exacerbated in the 9/11-era as discourse regarding terrorism has become more heavily focused on the use cyber space by terrorist organisations.[56]

[52] *Ibid.*

[53] *Ibid.*

[54] *Ibid.*

[55] G. Weimann, 'Cyberterrorism: How Real is The Threat?', *United States Institute of Peace*, December 2004, https://www.usip.org/sites/default/files/sr119.pdf, accessed 4 September 2016, pp. 2-3.

[56] *Ibid.*

Rhetoric which heightens public anxiety regarding the threat of cyberterrorism has been a major challenge for threat assessment in the public discourse. In 2012, speaking of the effect of a major cyberattack, former US Secretary of Defence Leon E. Panetta stated it could result in a:

> Cyber-Pearl Harbor that causes physical destruction and the loss of life, an attack that would paralyse and shock the nation and create a profound new sense of vulnerability.[57]

Hyperbole like this only serves to raise angst regarding cyber threats within society. This is not to say that cyber threats are not real, it is important to remain vigilant but governments and analysts should be averse to anxiety-driven hyperbole in addressing this threat publicly.[58]

Balancing messaging regarding threats, which alleviates public anxiety whilst being transparent about the high risk of cyber threats and already-compromised state of cybersecurity is a major challenge as well.[59] Gaps in threat assessment proves to be a challenge in future for cyber governance, a state which underestimates the risk associated with a cyber threat could have severe consequences for their cyber defence capabilities and ability to deliver strong cyber policy. Whilst, some states are prone to underestimating threats, Austin and Slay argue that one of the most pressing threat-based issues in contemporary cyber governance are the threat of complex, large-scale cyberattacks on national critical infrastructure, which could lead to a so-called "cyber armageddon."[60] They are concerned with the notion that increased reliance on artificial intelligence for autonomous

[57] E. Bumiller, T. Shanker, ‘Panetta Warns of Dire Threat of Cyberattack on US’, *New York Times*, 11 October 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=1, accessed 5 September 2016.

[58] P.W. Singer, 'The Cyber Terror Boogeyman', *Brookings Institution*, 1 November 2012, https://www.brookings.edu/articles/the-cyber-terror-bogeyman/, accessed 10 September 2016.

[59] C. Leuprecht, D.B. Skillicorn, V.E. Tait, ‘Beyond the Castle Model of cyber-risk and cyber-security’, *Government Information Quarterly*, Elsevier, 2016, pp. 1-3.

[60] G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security*, May 2016, p. 7.

decision-making is creating new vulnerabilities to cyberattacks.[61] Instead of focusing on actors as threats, Austin and Slay are more interested in examining the developments and estimations regarding future technologies of attack and defence systems and their potential vulnerabilities.[62]

Furthermore, they believe the level of concern for incorrect threat assessment is amplified given the fact that the Obama Administration declared a national emergency in cyberspace in both 2015 and 2016.[63] The fact that the administration stated that there were significant malicious cyber-enabled activities that originated internationally which continue to pose an extraordinary threat to US national security is enough evidence to suggest that serious concern should be taken regarding potential high-level cyberattacks. Because they see Obama's rhetoric as an omission that a major power has failed to secure its main cyber space assets, they rate the threat of cyber-attacks extremely high.[64]

COORDINATED INSTITUTIONAL STRUCTURE

The second category of analysis is coordinated institutional structure. This refers to the ability for states to implement a cohesive institutional structure of cyber-related departments and agencies, which will result in strong cyber maturity. The major components necessary for developing an institutional structure, which will result in strong cyber maturity, include a centralized cyber structure, which encourages a coordinated whole-of-government approach, which integrates numerous agencies of government such as intelligence agencies, law enforcement and defence.[65] Other components necessary for cyber maturity includes a

[61] *Ibid.*

[62] *Ibid.*

[63] *Ibid*, pp. 7-8.

[64] *Ibid.*

[65] T. Feakin, P. Jennings, 'The Emerging Agenda for Cybersecurity', *Australian Strategic Policy Institute*, July 2013, pp. 1-3.

commitment by states to international cooperation on cybersecurity [66] and CERT engagement.[67]

Strong cyber maturity within a state’s cyber institutions is demonstrated by the consolidation of departments and agencies into a coordinated, cohesive whole-of-government approach, which is centralized in power.[68] Feakin and Jennings believe that the consolidation of cyber departments at an operational level to centralize and strengthen national cyber capabilities whilst developing a whole-of-government approach will result in cyber maturity. The goal of the centralization is to decrease the potential for inter-departmental tension between cyber branches over whose responsibility it is to respond to cyber threats.[69] Some states have attempted to consolidate their cyber branches even more so by creating an executive position for an individual to preside over these centralized branches, such as a Cyber Czar.[70] In their research, Robinson, Gribbon, Horvath and Robertson have identified that almost all countries utilize an inter-departmental model of response to cybersecurity.[71] Consolidation and centralization of cyber institutions into a whole-of-government approach is the primary component needed for a coordinated institutional structure.[72]

A secondary component within a state’s institutional structure essential for cyber maturity is international engagement.[73] ASPI has suggested that international engagement is extremely

[66] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2015', *Australian Strategic Policy Institute*, 2015, p. 7.

[67] *Ibid.*

[68] T. Feakin, P. Jennings, 'The Emerging Agenda for Cybersecurity', *Australian Strategic Policy Institute*, July 2013, pp. 1-3.

[69] *Ibid.*

[70] *Ibid.*

[71] L. Gribbon, V. Horvath, K. Robertson, N. Robinson, 'Cyber-security Threat Characterisation: A Rapid Comparative Analysis', RAND Corporation, 2013, p. ix.

[72] T. Feakin, P. Jennings, 'The Emerging Agenda for Cybersecurity', *Australian Strategic Policy Institute*, July 2013, pp. 1-3.

[73] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2015', *Australian Strategic Policy Institute*, 2015, p. 7.

beneficial for a state's cyber governance and will result in cyber maturity[74] International engagement is primarily orchestrated by states who have a high degree of cyber maturity, these states have encouraged multilateral gatherings as a way of campaigning for strengthening cyber diplomacy to neutral states.[75] An example of strong international engagement in the Asia-Pacific in 2015 was the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.[76] Other international organizations shown to enhance global cyber engagement include The UN Internet Governance Forum, Asia-Pacific Computer Emergency Response Team (AP CERT) and the European Network Information Security Agency (ENISA).[77]

Third, a necessary component of attaining strong cyber maturity is engagement between CERT.[78] CERT is the name given to organized expert groups whose role is to respond to computer security threats, these groups exist within both a national and international capacity.[79] CERT engagement is an effective means to build the cybersecurity awareness and skills of less developed states as well as potentially easing strained cyber relations between states.[80] In relation to countering cybercrime, CERT engagement saw an improvement in regional cybercrime cooperation in 2015. It is likely that that CERT engagement will see a growth in cooperation between regional partners in countering cybercrime.[81]

[74] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2015', *Australian Strategic Policy Institute*, 2015, p. 7.
[75] *Ibid.*
[76] *Ibid.*
[77] 'Organizations and Institutions that Address International Cybersecurity', *Information Technology Industry Council*, 2016, http://www.itic.org/dotAsset/c/c/cc91d83a-e8a9-40ac-8d75-0f544ba41a71.pdf, accessed 10 September 2016.
[78] *Ibid.*
[79] K.R. Van Wyk, R.D. Pethia, 'Computer Emergency Response – An International Problem', Computer Emergency Response Team, Software Engineering Institute, *Carnegie Mellon University*, 1990, pp. 2-3.
[80] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2015', *Australian Strategic Policy Institute*, 2017, p. 7.
[81] T. Feakin, P. Jennings, 'The Emerging Agenda for Cybersecurity', *Australian Strategic Policy Institute*, July 2013, pp. 6-7.

The major challenge for implementing a coordinated institutional structure is the risk of a lack of cohesion within an institutional structure with an overabundance of cyber departments. Feakin and Jennings have argued that an overabundance of government and private sector entities has created an unnecessary convolution to cyber policy development.[82] This can lead to the possibility of interdepartmental tension, which is why it is so necessary to centralize and coordinate cyber institutions with a whole-of-government approach.[83]

COHERENT CYBER POLICY

The third category of analysis is coherent cyber policy. This refers to the ability for states to develop a coherent national cyber policy, which stems from its institutional structure, which informs cyber maturity. As technology has grown rapidly globally, governments have been forced to develop strong national cyber policy which safeguards against the cyber threats which rapid technological growth brings.[84]

A priority component for states wanting to develop coherent cyber policy is the establishment of a centralized national cybersecurity strategy, which is designed to develop cyber policy directives.[85] This is because they aim to give a clear, coherent national direction of the state's cyber policy objectives. Ariely argues that some of these strategies are indicative of cyber posturing by nation states on the global stage and that the majority of strategies converge internationally.[86] In terms of creating a cybersecurity strategy, Ariely argues that a convergence of multiple theoretical perspectives across the public and private sectors as well as defence departments is beneficial for creating a coherent cyber policy.[87]

[82] *Ibid.*
[83] *Ibid.*
[84] A. MacGibbon, 'Cyber Security: Threats and Responses in the Information Age', *Australian Strategic Policy Institute*, December 2009, Issue 26, pp. 1-6.
[85] A. Ariely, 'Adaptive Responses to Cyberterrorism', Cyberterrorism: Understanding, Assessment, and Response, Springer Publishing, 2014, pp. 180-181.
[86] *Ibid.*
[87] *Ibid*, pp. 181-182,

One major component of developing coherent cyber policy is the implementation of strong critical infrastructure protection (CIP).[88] This refers to the protection of physical facilities, supply chains, IT and communication networks that states rely on. CIP is a way of safeguarding against vulnerabilities, which cyberterrorists might want to take advantage of through a potential DDOS attack or through attacking the information systems of physical facilities such as water or power supply networks.[89] The responsibility of CIP is primarily undertaken by national CERT. Feakin and Jennings believe that it is imperative that governments improve this area of cyber policy to safeguard themselves from vulnerabilities and threats.[90] It is their belief that the critical infrastructure of a state is its life support system but that it is vulnerable to malicious cyberattacks.[91]

Private sector engagement is another necessary component for coherent cyber policy which in turn informs cyber maturity. ASPI has suggested that deeper government engagement with the private sector on cyber security.[92] Feakin and Jenning argue that by developing clearer mechanisms to collaborate with the private sector on cyber issues, it will create a greater ability to harness its skills and capacities to strengthen resilience against the threat of cyberterrorism.[93]

Third, an essential component for coherent cyber policy is the implementation of strong national cyber education programs, which range from tertiary to public awareness. Austin and Slay argue that the establishment of education institutions such as national cybersecurity

[88] A. MacGibbon, 'Cyber Security: Threats and Responses in the Information Age', *Australian Strategic Policy Institute*, December 2009, Issue 26, p. 10.

[89] *Ibid.*

[90] T. Feakin, P. Jennings, 'The Emerging Agenda for Cybersecurity', *Australian Strategic Policy Institute*, July 2013, pp. 6-7.

[91] *Ibid.*

[92] *Ibid*, p. 8.

[93] *Ibid.*

colleges will contribute to seeing gaps in cyber security policy reduced.[94] It is argued that effective cyber education policy would go a long way in terms of creating stronger cyber risk awareness and risk reduction measures.[95] A growing trend of governments is the creation of national cybersecurity centres in an effort to create effective policy and defence against cyber threats but also to create better public awareness and education regarding these threats.[96] In reference to Australia, Dupont has argued that cybersecurity centres are a worthwhile effort but a 'cradle to grave' educational investment is needed to improve cyber maturity to counter cyber threats. Dupont calls for cyber education starting at primary school in Australia, stating that cyber literacy must become an intuitive and foundational skill for Australians.[97]

Finally, dedicating a significant budgetary allocation to cyber governance is necessary for developing a coherent cyber policy, which will result in cyber maturity.[98] A well-funded model of cyber governance will result in greater cyber maturity as it will enhance the possibility for better national cyber infrastructure and capabilities.[99] Hawkins and Nevill argues itis essential as it allows governments to address international cybersecurity challenges such as conflict prevention frameworks, capacity building efforts, internet government initiatives and international cybercrime engagement.[100]

A major challenge for implementing a coherent cyber policy is the fact that states do not have the ability to completely govern the internet. For states which champion norms such as a free and open democratized internet, there cannot be any centralized control, which thus creates a

[94] G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security*, May 2016, pp. 16-20.

[95] *Ibid.*

[96] A. Dupont, 'Cybersphere is the Globe's New Battlefront', *The Lowy Institute*, 26 April 2016, http://www.lowyinstitute.org/publications/cybersphere-globes-new-battlefront, accessed 24 September 2016.

[97] *Ibid.*

[98] Z. Hawkins, L. Nevill, 'National cyber budgets', same, same but different', *Australian Strategic Policy Institute*, 16 June 2016, https://www.aspistrategist.org.au/national-cyber-budgets-different/, accessed 20 September 2016.

[99] *Ibid.*

[100] *Ibid.*

challenge for cyber governance.[101] A challenge for states in creating cyber policy is the fact that there are incentives for groups to resist measures governments make to secure the internet. These challenges come from groups such as privacy advocates, business interests, libertarians and technical purists who often have competing interests to states regarding cyber policy.[102]

ESTABLISHMENT OF CYBER DEFENCE RESPONSIBILITY

Fourth, the last category of analysis is the establishment of cyber defence responsibility. This refers to the ability for states to develop a system of cohesive, shared cyber defence responsibility, which encourages healthy cooperation between agencies affiliated with national cybersecurity. It is dependent on a number of factors with includes interagency cooperation, both shared and understood jurisdiction on cyber defence and information sharing between agencies. Although cyber defence responsibility promotes healthy cooperation between all agencies responsible for national cybersecurity, it is understood that intelligence agencies are best suited to undertake the primary role of leading national cyber defence compared to law enforcement and defence.[103]

The key component for establishing shared cyber defence responsibility is healthy inter-agency cooperation between intelligence, law enforcement and defence departments. Healthy inter-agency cooperation is essential for a shared burden of cybersecurity in which the responsibility of cybersecurity does not fall on a single branch or agency.[104] Finklea states that global efforts to improve inter-agency cooperation between intelligence and law enforcement agencies have included establishing interagency agreements over jurisdiction

[101] J.A. Hunker, T.K. Kelly, 'Cyber Policy: Institutional Struggle in a Transformed World', *I/S: A Journal of Law and Policy for the Information Society*, Vol. 8, No. 2, Fall 2012, pp. 214-215.
[102] *Ibid*, p. 216.
[103] B. Akhgar, F. Bosco, A. Staniforth, Cyber Crime and Cyber Terrorism Investigator's Handbook, Syngress, pp. 40-41.
[104] K.M. Finklea, ‘The Interplay of Borders, Turf, Cyberspace and Jurisdiction: Issues Confronting U.S. Law Enforcement’, *Congressional Research Service*, 17 January 2013, pp. 20-24.

inter-agency task forces and fusion centres, which assist in information sharing capabilities between agencies.[105] Regarding interagency cooperation, Von Knop has suggested that a paradigm shift is needed where the burden of cyber defence moves away from a hierarchal system in which responsibility falls on a single agency. She contends that this should be replaced by a networked system in which intelligence and law enforcement agencies should be linked according to a paradigm that relies on open and adaptive systems that promote learning, cooperation and flexibility.[106]

Within a culture of shared inter-agency cooperation, it is recognized that intelligence agencies are best suited to undertake lead responsibility of cyber defence, compared to law enforcement and defence.[107] According to Akhgar, Bosco and Stanisforth, intelligence agencies have been at the forefront of responding to cyberterrorism because terrorism has a different set of motivations and outcomes compared to other forms of crimes. Efforts against cyber threats and cyberterrorism are traditionally led by intelligence agencies because they undertake "higher policing" responsibility.[108] Despite intelligence being best suited for cyber defence, shared inter-agency cooperation is essential for establishing cyber defence responsibility, which will result in cyber maturity.

The biggest challenge to implementing an establishment of cyber defence responsibility is disagreement between agencies and competition for jurisdiction over cyber responsibility. Finklea argues that barriers in combatting cyber threats on a national and transnational level for intelligence and law enforcement agencies have included jurisdictional battles,

[105] *Ibid,* pp. 25-34.

[106] K. Von Knop, 'Institutionalization of a Web-Focused, Multinational Counter-Terror Campaign', Responses to Cyber Terrorism', *Centre of Excellence Defence Against Terrorism*, 2008, p.16.

[107] B. Akhgar, F. Bosco, A. Staniforth, Cyber Crime and Cyber Terrorism Investigator's Handbook, Syngress, pp. 40-41.

[108] *Ibid.*

investigative overlaps and in inability so share information. [109] This is why the implementation of inter-agency task forces, fusion centres and outlining clear cyber defence jurisdiction is essential for cyber maturity.[110]

A secondary challenge for establishing shared cyber responsibility is the excessive growth in cyber militarization. A growing trend is that as cyber threats grow, national defence departments are developing their cyber capabilities exponentially. This is because cyber threats often come from international actors which domestic law enforcement is often powerless to deter or punish.[111] As cyber capabilities within defence departments grow, these capabilities are increasingly being hidden from public view, which makes research on this field difficult and indicates a lack of transparency within cyber governance.[112] Furthermore, Wallace issues caution with defence departments undertaking too much cyber responsibility because it runs the risk of a state depending too heavily on the military for cybersecurity, which in turn may reduce the incentives for the private sector and law enforcement to develop long-term solutions to cyber threats.[113] Defence departments are essential to national cyber defence but they are not suited to undertake primary responsibility, they are best utilized in a system of shared cooperation with other agencies.[114]

[109] K.M. Finklea, ‘The Interplay of Borders, Turf, Cyberspace and Jurisdiction: Issues Confronting U.S. Law Enforcement’, *Congressional Research Service*, 17 January 2013, pp. 20-24.

[110] *Ibid.*

[111] I. Wallace, 'The Military Role in National Cybersecurity Governance', *Brookings Institution*, 16 December 2013, https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/, accessed 23 September 2016.

[112] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2015', *Australian Strategic Policy Institute*, 2015, pp. 6-7.

[113] I. Wallace, 'Cyber Security: Why Military Forces should take a Back Seat', *The Lowy Interpreter*, 21 October 2013, http://www.lowyinterpreter.org/post/2013/10/21/Cyber-security-Why-military-forces-should-take-a-back-seat.aspx, accessed 23 September 2016.

[114] *Ibid.*

CONCLUSION

This chapter has identified a framework for analysis comprising four key categories in which to analyse contemporary cybersecurity as it responds to cyber threats. These are: accurate threat analysis, coordinated institutional structure, coherent cyber policy, and the establishment of cyber defence responsibility. All of these components are essential in gauging the maturity of a state's cyber capabilities in deterring and responding to threat. One of the most striking points when analysing the current threats associated with state and non-state actors is that there is a perceived lack of awareness of the danger, risks and associated likelihood. Threats range from high-risk to low-risk and are analysed often in terms to the potential damage they can do the critical infrastructure. The major challenge for accurate threat analysis is striking the right balance being able to evaluate the risk of the cyber threat and the actor responsible whilst creating public messaging, which does not cause unreasonable alarm whilst being transparent about the risks and realities regarding cyber threats that society faces. A common trend across these areas in response to these concerns is the emphasis for improved education, centralization and engagement within the domestic community and internationally. All factors focus on providing better education for cyber awareness, centralizing cyber policy as a whole-of-government approach and engaging international actors and the private sector through cooperation. Overall, the analysis in this chapter has found that a whole-of-government approach to cyber governance, international cyber cooperation, CIP, private sector cooperation and cyber education are essential components needed for states to attain strong cyber maturity. These components comprise a framework to examine how Australia and the US have responded domestically to cyberterrorism as well as cooperating with one another in response to cyber threats.

CHAPTER TWO:
The Quick Growth of Australia's Cyber Maturity

INTRODUCTION

In this chapter, Australia's cyber maturity will be evaluated using the four categories of the theoretical framework. The framework, suggests that a combination of a whole-of-government approach with a focus on CERT infrastructure and international engagement will create strong cyber maturity.[115] It also indicates the importance of investment in private sector and public education whilst maintaining a healthy balance of cyber defence responsibility.[116] It can also be ascertained that Australia has made significant progress in recent years to address its lag in cybersecurity. The Australian government has made an effort to follow the institutional structure of western states with more sophisticated cyber institutions and policy like the US and Western European states.[117]

Australia is not immune from cyberattacks and faces the same threats as other western states.[118] Australia's major challenge in the future is continually improving upon its cybersecurity efforts as a core security issue.[119] Nonetheless, given the vulnerabilities, Australia can stand to improve its cybersecurity, and it can do so with greater investment and focusing on strengthening its threat awareness, CERT defence capabilities and by further committing to cyber education within a range of public sectors.[120]

[115] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2016, *Australian Strategic Policy Institute*, 2016, pp. 6-9.

[116] G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security*, May 2016, pp. 12-22.

[117] *Ibid*, pp. 1-7.

[118] *Ibid*, pp. 7-10.

[119] *Ibid*, pp. 10-12.

[120] *Ibid*, pp. 20-22.

AUSTRALIA AND ACCURATE THREAT ANALYSIS

The aim of this category is to evaluate Australia's current cyber threat challenges. In terms of priorities for national security, Australia currently evaluates the threat of state-based cyberattacks higher than non-state cyberterrorism.[121] Australia's threat analysis is consistent with current cyber expert analysis.[122] There is a high emphasis on the threat of cyberattacks which can cause major damage to critical infrastructure such as DDOS attacks, state-based espionage, cyberattacks which target financial systems above the internet being used as a recruitment tool by terrorist organisations.[123] Whilst making it known that the threat of cyberterrorism is real, the Australian government has attempted to reduce public anxiety by bringing attention to the lack of cyber terrorist organisation capabilities.[124]

The major priority for Australia in accurate threat analysis is state-based cyber threats. A major event which has caused the Australian government to focus on state-based cyber espionage was the 2015 Bureau of Meteorology (BOM) attack which illustrated Australia's potential vulnerability to foreign espionage and state-sponsored cyberattacks. In 2015, the BOM computer network was infiltrated by state-based hackers which the ABC allegedly traced back to China.[125] It is alleged that the motivations behind this attack were BOM's network's interconnections with other government departments such as the Department of

[121] Australian Cyber Security Centre, 2016 Threat Report, Australian Federal Government, 2016, pp. 5-9.
[122] L. Gribbon, V. Horvath, K. Robertson, N. Robinson, 'Cyber-security Threat Characterisation: A Rapid Comparative Analysis', *RAND Corporation*, 2013; G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security*, May 2016; Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2015', *Australian Strategic Policy Institute*, 2015; A. MacGibbon, 'Cyber Security: Threats and Responses in the Information Age', *Australian Strategic Policy Institute*, December 2009, Issue 26; T. Feakin, P. Jennings, 'The Emerging Agenda for Cybersecurity', *Australian Strategic Policy Institute*, July 2013; P.W. Singer, 'The Cyber Terror Boogeyman', *Brookings Institution,* 1 November 2012, https://www.brookings.edu/articles/the-cyber-terror-bogeyman/, accessed 10 September 2016.
[123] *Ibid.*
[124] *Ibid*, pp. 8-9.
[125] Uhlmann, C., 'China blamed for 'massive' cyber attack on Bureau of Meteorology computer', *ABC News*, 2 December 2016, http://www.abc.net.au/news/2015-12-02/china-blamed-for-cyber-attack-on-bureau-of-meteorology/6993278, accessed 7 November 2016.

Defence.[126] In 2016 the Australian Cyber Security Centre (ACSC) Threat Report stated that Australia continues to be a target of persistent and sophisticated cyber espionage.[127] Despite the fact that more foreign states have acquired or are acquiring cyber espionage capabilities, the ACSC maintains that it is aware of diverse state-based adversaries attempting cyber espionage against Australian systems strategic, operational and commercial intelligence requirements.[128] They evaluate that cyber espionage poses more of a threat to national cyber infrastructure, the protection of sensitive government information, the private sector and the defence and intelligence community than non-state cyberterrorism currently.[129] Despite this ongoing threat, the ASCS claims that frequency of detected cyber espionage is miniscule in comparison to the size of Australia's government and non-government cyber infrastructure.[130] This can be viewed as an effort to reduce public anxiety regarding cyberattacks, something which Singer has claimed is essential for cyber maturity.[131]

Secondary threats for Australia's intelligence and defence community lie in the realm of non-state cyberterrorism. The Cyber Threat Report states that terrorist groups that seek to harm Western interests currently pose a low cyber threat.[132] When analysing the threat level associated with these groups, Australia has faced minor cyberattacks from non-state cyberterrorists. In 2015, the Islamic State (IS) followers were able to hack the personnel information of Australian Defence Force employees, a Victorian MP and several public servants.[133] The Islamic State Hacking Division released their personal information, which

[126] Besser, L., Stumer, J., Sveen, B., ‘Government computer networks breached in cyber attack as experts warn of espionage threat’, *ABC News*, 29 August 2016, http://www.abc.net.au/news/2016-08-29/chinese-hackers-behind-defence-austrade-security-breaches/7790166, accessed 7 November 2016.

[127] Australian Cyber Security Centre, 2016 Threat Report, Australian Federal Government, 2016, pp. 5-7.

[128] *Ibid.*

[129] *Ibid*, pp. 1-9.

[130] *Ibid.*

[131] P.W. Singer, 'The Cyber Terror Boogeyman', *Brookings Institution*, 1 November 2012, https://www.brookings.edu/articles/the-cyber-terror-bogeyman/, accessed 10 September 2016.

[132] Australian Cyber Security Centre, 2016 Threat Report, Australian Federal Government, 2016, pp. 8-9.

[133] Bucci, N., ‘Islamic State posts Australian hit list after hacking addresses, mobile numbers’, 12 August 2015, http://www.smh.com.au/national/islamic-state-posts-australian-hit-list-after-hacking-addresses-mobile-numbers-20150812-gixrmz.html, accessed 7 November 2016.

included mobile phone numbers, emails addresses and online passwords, and encouraged home-grown terrorists to assassinate these individuals.[134] This attack can be interpreted as a propaganda tool with the intent to recruit, radicalize and mobilize home-grown terrorists alongside creating a sense of fear and anxiety amongst the Australian public.[135]

The ACSC states that the cyber abilities of terrorist groups remain rudimentary and show few signs of improving significantly in the near future. The ACSC believes that the major focus of cyberterrorists are DDOS attacks, hijacking social media accounts, defacing websites, the hack and release of personal information and compromising poorly-secured internet-connected services.[136] Furthermore, the report states that it is possible that terrorist groups could potentially develop more sophisticated cyber capabilities but it is unlikely they will be able to disrupt a secure network and create a disruptive or destructive effect in the next two to three years. Instead they are more likely to focus on embarrassing governments, imposing financial costs and achieving propaganda and recruitment victories.[137] Despite being a secondary priority, the Australian intelligence community has assessed that the threat of non-state cyberterrorism is on the rise.[138] Former Australian Security Intelligence Organisation (ASIO) Director-General David Irvine has raised concerns about the growing threat of online Jihadists' abilities to launch powerful cyberattacks stating that:

> While terrorist organisations have not yet exhibited sophisticated cyberattack capability, we must anticipate, given the sophistication they demonstrated in using the internet for propaganda and other reasons that

[134] *Ibid.*

[135] United Nations Office on Drugs and Crime, 'The Use of the Internet for Terrorist Purposes', *United Nations*, 2012, pp. 3-6.

[136] Australian Cyber Security Centre, 2016 Threat Report, Australian Federal Government, 2016, pp. 8-9.

[137] *Ibid.*

[138] D. Wroe, 'Jihadists could launch major cyber attacks, says former ASIO boss David Irvine', in *Sydney Morning Herald*, 26 October 2016, http://www.smh.com.au/federal-politics/political-news/jihadists-could-launch-major-cyber-attacks-says-former-asio-boss-david-irvine-20151026-gkisup.html, accessed 7 November 2016.

> they could well seek to develop destructive attack capabilities in the near term.[139]

Despite the possibility of non-state actors being able to commit sophisticated cyberattacks rising, the use of the internet as a propaganda device is the currently biggest threat faced from traditional terrorist groups.[140]

The biggest challenge currently for Australia's ability to accurately analyse cyber threats is providing a transparent and realistic threat assessment balanced with public messaging which doesn't unnecessarily heighten anxiety regarding cyberterrorism. Australia has attempted to avoid raising public fears of the threat of cyberterrorism whilst also presenting a realistic analysis of the growing threats associated with terrorist use of the internet.[141] This approach falls in line with Singer's belief fears of cyberterrorism are largely being overblown and contributing to societal anxiety regarding these threats.[142] Some experts have also argued that the language used by the Australian government regarding threat assessment is too broad, non-specific and falls back on exhausted cyber policy generalizations.[143] Austin has argued that there is a gap between the language used by Australia and international allies rhetorically, whereby the Australian government vaguely refers to "significant cyber events" and "terrorism" without specifically referring to the contemporary threats which state-actors pose such as attacks on critical infrastructure.[144] Furthermore, Austin criticizes the strategy for failing to mention the threat posed by state sponsored cyber espionage, which should be a high priority for the Australian Government. Austin also believes that the Australian

[139] *Ibid.*
[140] *Ibid.*
[141] P.W. Singer, 'The Cyber Terror Boogeyman', *Brookings Institution*, 1 November 2012, https://www.brookings.edu/articles/the-cyber-terror-bogeyman/, accessed 10 September 2016.
[142] *Ibid.*
[143] G. Austin, 'Australia still doesn't see a cyber attack as the menace our allies fear', *The Conversation*, April 25 2016, https://theconversation.com/australia-still-doesnt-see-a-cyber-attack-as-the-menace-our-allies-fear-57719, accessed 10 November 2016.
[144] *Ibid.*

government has presented an anodyne narrative to the Australian public which underestimates the current threats associated with cyberattacks. This illustrates that despite it largely showing signs of strong cyber maturity, Australia still needs to develop a sophisticated dialogue with the Australian public regarding cyber threats.[145]

Other contemporary perspectives suggests a more concerning set of circumstances. In line with Leuprecht's view,[146] Rogers states that there has been a paradigm shift in which the focus shifted from trying to defend networks from attack to defending the information stored within a network.[147] There should now be an assumption that government and private sector digital data security is breached. They are at a permanent structural disadvantage due to exponential threats such as malware, known vulnerabilities zero day exploits or existing but unknown vulnerabilities.[148] This analysis, which suggests a concerning scenario regarding a high level of threat vulnerability, is in line with Austin's critique that Australia's current threat analysis publically underestimates the severity of cyber threats it faces.[149]

AUSTRALIA AND COORDINATED INSTITUTIONAL STRUCTURE

The aim of the following section is to analyse Australia's ability to develop a coordinated institutional structure. Australia has attempted to develop a centralized, whole-of-government approach across several different government agencies and departments.[150] Within this whole-of-government approach, Australia has attempted to engage with the private and educational sector as well as CERT agencies. Australia has attempted to engage

[145] *Ibid.*
[146] C. Leuprecht, D.B. Skillicorn, V.E. Tait, 'Beyond the Castle Model of cyber-risk and cyber-security', *Government Information Quarterly,* Elsevier, 2016, pp. 1-3.
[147] Z. Rogers, 'ASCS 2017 Report: Australian Cyber Security Centre Conference", *Flinders University Centre for United States and Asia Policy Studies,* 20 March 2017, p. 1.
[148] *Ibid,* Pp. 1-2.
[149] G. Austin, 'Australia still doesn't see a cyber attack as the menace our allies fear', *The Conversation*, April 25 2016, https://theconversation.com/australia-still-doesnt-see-a-cyber-attack-as-the-menace-our-allies-fear-57719, accessed 10 November 2016.
[150] T. Feakin, P. Jennings, 'The Emerging Agenda for Cybersecurity', *Australian Strategic Policy Institute,* July 2013, pp. 1-3.

internationally with other states and global cyber institutions on cybersecurity which is essential to creating strong cyber maturity in domestic cyber institutions.[151]

The Australian cyber governance institution which most represents its commitment to a whole-of-government approach is the ACSC. The ACSC was created with the goal of consolidating and bringing together Australia's various cyber branches and agencies such as the Defence Department, Attorney-General's Department, ASIO, Australian Federal Police (AFP) and the Australian Crime Commission into a single location.[152] Its role is to lead Australia's operational response spread across this consolidation of branches to cybersecurity incidents, organise national cybersecurity operations and resources, to study and investigate cyber threats as well as raising national awareness regarding cyber threats. Encompassing a whole-of government approach, the ACSC's goal is to centralize government branches from a number of different backgrounds and traditions like intelligence, policymaking, law enforcement and defence into contributing to cybersecurity infrastructure.[153] The ACSC is also committed to building upon already strong links between the Australian government and the private sector.[154] Figure 2.1 illustrates the efforts by the Australian government to develop a whole-of-government approach to cyber governance.

[151] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2016, *Australian Strategic Policy Institute*, 2016, pp. 6-9.
[152] T. Feakin, P. Jennings, 'The Emerging Agenda for Cybersecurity', *Australian Strategic Policy Institute*, July 2013, p. 2.
[153] *Ibid.*
[154] Australian Cyber Security Centre, 'Frequently-Asked Questions', *Commonwealth of Australia 2016*, https://www.acsc.gov.au/faqs.html, accessed 4 November 2016.

Figure 2.1: Australian Institutional Structure of Cyber Governance

Figure removed due to copyright restriction

Source: Feakin, T., and Jennings, P., 'The Emerging Agenda for Cybersecurity', Australian Strategic Policy Institute, July 2013, p. 3.

Research in Chapter One highlights the importance of the implementation of strong critical infrastructure protection within a coordinated institutional structure. The ACSC strives to achieve this by working in consultation with CERT Australia. CERT Australia is the national computer response team and it is the main point of contact within the government for Australian businesses for issues related to cybersecurity.[155] It is their primary role to provide advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure i.e. businesses.[156] In addition to direct working relationships with the private sector, CERT Australia also shares information on matters of cybersecurity

[155] Attorney-General’s Department, ‘CERT Australia: About us’, *Commonwealth of Australia 2016*, https://www.cert.gov.au/about, accessed 4 November 2016.

[156] *Ibid.*

with ASIO, AFP, Australian Signals Directorate (ASD), and the Defence Intelligence Organisation (DIO).[157] The 2016 ASPI Cyber Maturity report graded both Australia's ability to govern on matters of cybersecurity and CERT capabilities as an 8. This illustrates that Australia's efforts to create strong institutional structures are in accordance with current theoretical perspectives on what constitutes strong cyber maturity.[158]

International engagement has been cited by experts as one of the key factors in producing strong cyber maturity, Australia has taken effective action to create cooperation, relationships and engagement with both allies and neutral states in the international community.[159] Australia's international cybersecurity relationships are predominantly defined by their membership in intelligence alliances and treaties, particularly as it pertains to combatting the threat of cyberterrorism.[160]

The treaty which most emboldens Australia's commitment to international cooperation on cybersecurity in terms of intelligence is the UKUSA (Five Eyes) Treaty. Five Eyes is an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States.[161] Broadly speaking, Five Eyes is a multilateral treaty for joint cooperation in signals intelligence. Five Eyes was originally used as a surveillance mechanism for allied states to monitor private communications of the former Soviet Union and the Eastern Bloc.[162] Following the September 11 attacks, Five Eyes focused its surveillance primarily on

[157] *Ibid.*
[158] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2016, *Australian Strategic Policy Institute*, 2016, p. 19.
[159] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2016, *Australian Strategic Policy Institute*, 2016, p. 19.
[160] Davies, A., Jennings, P., 'Expanding Alliance: ANZUS Cooperation and Asia-Pacific security', *Australian Strategic Policy Institute*, 2014, pp. 5-7.
[161] The Australian role is currently overseen by the ASD, the Treaty was signed in the post-war II period as part of the Atlantic Charter which set out Allies goals for the post-war world. See: Australian Signals Directorate, 'UKUSA Allies', *Commonwealth of Australia 2016*, 2016, http://www.asd.gov.au/partners/allies.htm, accessed 5 November 2016.
[162] Tanter, R., 'Fifty years on, Pine Gap should reform to better serve Australia', *The Conversation*, 9 December 2016, http://theconversation.com/fifty-years-on-pine-gap-should-reform-to-better-serve-australia-65650, accessed 10 December 2016.

monitoring the threat of terrorism during the War on Terror.[163] During this period, Five Eyes expanded its surveillance into the cyber territory by monitoring the threat of terrorism growth, planning and organization through internet usage.[164] This Treaty can be viewed as essential to Australia's international engagement in the intelligence and cyber community.[165]

Alongside Five Eyes, Australia's intelligence alliance with the US is strengthened by the ANZUS Treaty. The ANZUS Treaty is another example of Australia's commitment to international engagement in cybersecurity. The ANZUS Treaty is a collective security agreement between Australia, New Zealand and the US signed in 1951 which binds the three states to cooperate on military matters in the Pacific Ocean region.[166] Following the September 11 attacks the Treaty has been expanded so that the states are required to cooperate on military matters worldwide.[167] This Treaty is important in the scope of cyberterrorism for Australia in post 9/11 era. As the threat of terrorism rises globally, treaties such as ANZUS deepen relationships with strong allies such as the US. As the cyber sphere is being used more consistently as a vehicle of terrorism, the interpretation of the ANZUS treaty will be forced to respond and expand to these new threats.[168] This can only result from a deepening of the strategic alliance with the US and can only benefit Australia in safeguarding itself against the threat of cyberterrorism in the future. The ANZUS treaty can be understood

[163] N. Perry, P. Dodds, 'Five Eyes spying alliance will survive Edward Snowden: experts', *Sydney Morning Herald*, 18 July 2013, http://www.smh.com.au/it-pro/security-it/five-eyes-spying-alliance-will-survive-edward-snowden-experts-20130717-hv0xw.html, accessed 5 April 2017.

[164] B. Nicholson, 'Five Eyes saving lives', *The Australian*, 20 November 2013, http://www.theaustralian.com.au/news/inquirer/five-eyes-saving-lives/news-story/c365f88578b16a97b6e874c6c503b4ae, accessed 5 April 2017.

[165] Davies, A., Jennings, P., 'Expanding Alliance: ANZUS Cooperation and Asia-Pacific security', *Australian Strategic Policy Institute*, 2014, p. 22

[166] Davies, A., Jennings, P., 'Expanding Alliance: ANZUS Cooperation and Asia-Pacific security', *Australian Strategic Policy Institute*, 2014, pp. 5-7.

[167] '2016 Defence White Paper', *Commonwealth of Australia 2016*, p. 121.

[168] A. Davies, 'An Australian perspective on ANZUS and cyberthreats', ANZUS 2.0: Cybersecurity and Australia-US Relations, *Australian Strategic Policy Institute*, 2012, pp. 3-5.

as a strong example of Australia’s commitment to international cooperation on cybersecurity within the intelligence community.[169]

Alongside intelligence alliances, Australia has gone to great lengths in recent years to commit to regional engagement on broader matters of cybersecurity. In its 2016 Cyber Maturity Report, ASPI allotted Australia a 9.0 score for its engagement in international discussions on cyberspace, including in bilateral, multilateral and other forums. It also recognised Australia’s willingness to champion a free, open and secure internet, preventing cybercrime; and building Asia-Pacific cybersecurity capacity.[170] Australia is making significant efforts to be more present in multilateral international discussions, coalitions and forums focused on regional cybersecurity in the Asia-Pacific.[171]

AUSTRALIA AND COHERENT CYBER POLICY

In its relative infancy, Australia has attempted to create a coherent cyber policy.[172] It has attempted to develop national cyber policy which is made up of components which includes the development of national security strategies,[173] prioritizes CIP,[174] engagement with the private sector[175] and investment in cyber education.[176] A cyber policy which attempts to engage with several different sectors is viewed as essential to strong cyber maturity.[177]

[169] D. Nichola, ‘Expanding Alliance: ANZUS Cooperation and Asia-Pacific security’, *Australian Strategic Policy Institute*, 2014, pp.20-22.

[170] Australian Strategic Policy Institute, ‘Cyber Maturity in the Asia-Pacific Region 2016, *Australian Strategic Policy Institute*, 2016, p. 19.

[171] ‘2016 Cyber Security Strategy’, *Commonwealth of Australia 2016*, pp. 39-43.

[172] ‘2016 Cyber Security Strategy’, *Commonwealth of Australia 2016,* pp. 4-11.

[173] A. Ariely, ‘Adaptive Responses to Cyberterrorism’, Cyberterrorism: Understanding, Assessment, and Response, Springer Publishing, 2014, pp. 180-181.

[174] A. MacGibbon, 'Cyber Security: Threats and Responses in the Information Age', *Australian Strategic Policy Institute,* December 2009, Issue 26, p. 10.

[175] T. Feakin, P. Jennings, 'The Emerging Agenda for Cybersecurity', *Australian Strategic Policy Institute,* July 2013, p. 9.

[176] G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security,* May 2016, pp. 16-20.

[177] G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security,* May 2016, pp. 16-20.

An example of Australia's commitment to developing coherent cyber policy is the 2016 Cyber Security Strategy.[178] This policy paper has indicated that the government intends to utilize a number of branches with a vast range of resources to assist and protect the online environment of the government, private sector and the Australian public.[179] As seen in Figure 2.2, the strategy prioritizes each of the components discussed in the framework essential for cyber maturity, there is a high emphasis on CIP and engagement with the private sector.[180] The policy directives in line with Chapter One's framework where the Australian government intends to enhance its cyber maturity are outlined in the figure below:

[178] *Ibid.*
[179] *Ibid.*
[180] *Ibid.*

Figure 2.2: Australia's Cyber Security Strategy 2016

Figure removed due to copyright restriction

Figure removed due to copyright restriction

Source: ‘2016 Cyber Security Strategy’, *Commonwealth of Australia 2016*, pp. 10-11.

As seen in Figure 2.2, the strategy has presented a set of policy initiatives for Australia's commitment to enhancing stronger cyber maturity where its components largely fall in line with Chapter One’s framework.[181] By placing the ACSC as the centralized institution of cybersecurity, the government has attempted to deliver policy which focuses heavily on CIP, engagement with the private sector and developing stronger cyber education.[182]

The Australian government has chosen to focus on education as a key pathway to ensuring cyber maturity. The plans for opening academic centres of cybersecurity excellence as well as promoting public education in cybersecurity are the primary methods in which the government is attempting to accomplish this goal.[183] The government's plan to focus on developing better nationwide education is in line with current theoretical perspectives which place a high value on investing in education as a successful means for promoting strong cyber governance. A better educated public on cybersecurity alongside investing in high-skilled cybersecurity professionals will do well to ensure Australia's strength in defending against the threat of cyber threats.[184]

The major challenge for the Australian government has been dedicating a significant amount of budgetary resources to cyber governance. In terms of cybersecurity resources, the Australian government announced within the cybersecurity strategy that they plan to invest approximately AUD230 million dollars into cybersecurity infrastructure. Mostly this investment will be directed into national cyber defences such as joint cyber threat sharing centres, CERT Australia, private sector engagement and increasing the government's cybercrime investigation and response capabilities.[185] This can be considered a landmark

[181] G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security*, May 2016, pp. 11-12.
[182] ‘2016 Cyber Security Strategy’, *Commonwealth of Australia 2016*, pp. 4-11.
[183] *Ibid*, pp. 51-55.
[184] *Ibid*.
[185] ‘Cyber-security strategy funding fact sheet’, *Commonwealth of Australia 2016*.

investment by the Australian government with expected direct benefits in Australia's defence against cyber threats.[186]

However, cyber experts have critiqued it as too small in comparison to international allies' cyber investment. Austin and Slay have pointed out that whilst the AUD230 million invested by the Turnbull government is impressive, it pales in comparison to the investment AUD24 billion by the US government as an emergency cybersecurity package just for 2017.[187] A criticism of the Cyber Security Strategy is an inadequate investment in cyber education, Austin and Slay believe that within the strategy, the commitment to cyber education does not go far enough and whilst the establishment of academic centres within universities is education is commendable, there is a need for further education investments such as TAFE courses in cybersecurity and a national cybersecurity college.[188]

AUSTRALIA AND ESTABLISHMENT OF CYBER DEFENCE RESPONSIBILITY

Australia has attempted to develop a clear establishment of cyber defence responsibility between its numerous agencies responsible for cybersecurity.[189] With a focus on improving inter-agency cooperation and information sharing amongst intelligence departments such as ASIO, AFP and the Australian Secret Intelligence Service (ASIS), Australia finds itself in a good position for attaining cyber maturity.[190]

[186] *Ibid.*

[187] G. Austin, 'Australia still doesn't see a cyber attack as the menace our allies fear', *The Conversation*, April 25 2016, https://theconversation.com/australia-still-doesnt-see-a-cyber-attack-as-the-menace-our-allies-fear-57719, accessed 10 November 2016.

[188] J. Slay, 'Australia is vulnerable to cyber threats, so what can we do about it', *The Conversation*, 12 October 2016, https://theconversation.com/australia-is-vulnerable-to-cyber-threats-so-what-can-we-do-about-it-66903, accessed 7 April 2017.

[189] B. Akhgar, F. Bosco, A. Staniforth, Cyber Crime and Cyber Terrorism Investigator's Handbook, Syngress, pp. 40-41.

[190] A.P. Wadell, 'Cooperation and Integration among Australia's National Security Community', *Studies in Intelligence*, Vol. 59, No. 3, September 2015, pp. 26-32.

A primary example of Australia's establishment of cyber defence responsibility, in addition to the ACSC, is the National Counter-Terrorism Plan (NCTP).[191] The performative function of the NCTP in countering online violent extremism as a propaganda, recruitment and coordination tool is essential to Australia's capabilities to defend against the broad spectrum of cyberterrorism.[192] The NCTP is a mechanism for shared responsibility and inter-agency cooperation between agencies responsible for cybersecurity and counter-terrorism.[193] As identified in Chapter One, traditional intelligence organisations such ASIO, ASIS and the AFP can appropriately undertake the majority of responsibility as it pertains to cyber defence.[194] They are best suited to respond the specificity of terrorist threats as they operate within the secretive and sensitive domain of national security.[195] Below, Figure 2.3 illustrates the healthy burden of cyber defence held by Australia's intelligence agencies as it shows their responsibility and jurisdiction to respond to certain types of cyber threats.

[191] National Counter-Terrorism Committee, 'National Counter-Terrorism Plan', *Commonwealth of Australia 2012,* pp. 3-6, 12-15.
[192] *Ibid.*
[193] *Ibid.*
[194] *Ibid.*
[195] *Ibid.*

Figure 2.3: Responsibilities of Australian Cyber Agencies

Figure removed due to copyright restriction

Source: Austin, G., and Slay, J., 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security*, May 2016, pp. 6-7.

Despite the challenge for governments to avoid becoming too reliant on cyber military capabilities,[196] Australia's shared establishment of cyber defence responsibility has currently avoided this risk. The ACSC's oversight of the ASD has meant that the department of

[196] I. Wallace, 'The Military Role in National Cybersecurity Governance', *Brookings*, 16 December 2013, https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/, accessed 23 September 2016.

defence is engaged within a system of inter-agency cooperation and information sharing with intelligence and law enforcement agencies.[197] Through a commitment to inter-agency cooperation and information sharing facilitated through the ACSC, the Australian government has balanced its investment in cyber military capabilities with maintaining a whole-of-government approach to cyber defence which encourages shared responsibility and cooperation across a number of agencies.[198] The role of the ASD is indispensable to Australia's cyber capabilities and ability to defend against cyber threats.[199] In 2016, Prime Minister Turnbull announced that the ASD will be utilizing their newly developed offensive cyber capabilities in the fight against IS in Syria and Iraq. The ASD will deploy their new technological capabilities from Canberra in order to support coalition military operations in this region, this is a landmark moment for attacking cyberterrorism on the offensive and for Australia's cyber capabilities.[200] The creation of these new cyber technologies illustrate how important defence is to Australia's cybersecurity future.[201]

CONCLUSION

Australia has largely made the right efforts in its relative infancy to establish successful cyber governance in line with the research offered in Chapter One. Australia has relatively well-developed cyber maturity but is exposed to clear vulnerabilities. It has prioritized the threat of state-based cyber espionage over non-state cyber terrorism as the biggest cyber threats that Australia currently faces. It has attempted to create cyber policy which focuses on improving CIP, engagement with a wide range of industry such as the private sector and education as

[197] Australian Signals Directorate, 'ACSC- Australian Cyber Security Centre', *Commonwealth of Australia 2017*, https://www.asd.gov.au/about/roleinfosec.htm, accessed 8 April 2017

[198] '2016 Cyber Security Strategy', *Commonwealth of Australia 2016*, pp. 4-11.

[199] Australian Signals Directorate, 'Information Security (Infosec) Role', *Commonwealth of Australia 2017*, https://www.asd.gov.au/about/roleinfosec.htm, accessed 8 April 2017.

[200] K. Murphy, 'Australia taking cyber fight to Isis, Malcolm Turnbull to confirm', *The Guardian*, 23 November 2016, https://www.theguardian.com/technology/2016/nov/23/australia-taking-cyber-fight-to-isis-malcolm-turnbull-to-confirm, accessed 8 April 2017.

[201] *Ibid.*

well as investing focusing on public awareness regarding cybersecurity. The creation of the ACSC, the 2016 Threat Report, and the 2016 Cyber Security Strategy have been landmark developments in the creation of infrastructure and policymaking which reinforces Australia's commitment to cybersecurity. Although these efforts are commendable, Australia’s cyber governance is not without its gaps. Australia has been criticized for underscoring the current threat level associated with cyberattacks in comparison to regional partners. There are concerns that Australia’s threat awareness is outdated, and it has failed to implement sufficient cyber defence measures. This is in line with Leuprecht’s view that current methods to prevent cyber threats are ineffective due to the fact that critical infrastructure may already be breached. Furthermore, experts have argued that Australia should be allocating more significant resources to improving its cybersecurity infrastructure and capabilities.

Chapter Three:
The Exponential Growth and Limits of US Cyber Primacy

INTRODUCTION

The US has long been viewed as a global pacesetter in cybersecurity and is considered to be the leading global actor in terms of cyber infrastructure and capabilities globally and within the Asia-Pacific.[202] The US has excelled at attaining cyber maturity as its national cyber infrastructure is amongst the most advanced in the world.[203] It has excelled at CERT infrastructure, international engagement, engagement with the private sector as well as creating a mammoth institutional cyber culture which utilizes a whole-of-government approach.[204] These factors lead to its sophisticated level of threat analysis which prioritizes the risk of state-based cyber threats.[205] Nonetheless, the US has become a target for cyber threats from state based cyberattacks and espionage as well as subject to non-state cyberterrorism. Overall, the US has done extremely well to ensure strong cyber maturity based on its whole-of-government institutional structure, a commitment to international cooperation which advocates for stronger digital diplomacy and cyber policy which has shown a commitment to CIP, private sector engagement and cyber education.

This chapter will evaluate US cyber maturity and its preparedness to respond to cyber threats by using the four categories of analysis established in Chapter One. In terms of accurate threat analysis, the major focus of western states is the threat of state-based threats balanced

[202] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2016', *Australian Strategic Policy Institute*, 2016, pp. 81-85.

[203] *Ibid.*

[204] *Ibid.*

[205] F.J. Cilluffo, 'Testimony on Emerging Cyber Threats to the United States before the US House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Securities Technology', 2016, http://docs.house.gov/meetings/HM/HM08/20160225/104505/HHRG-114-HM08-Wstate-CilluffoF-20160225.pdf, accessed 10 December 2016, pp. 1-4.

with the growing risk of non-state cyberterrorism.[206] A common analytical theme is the attempt to develop an institutional structure which utilizes a whole-of-government approach, international cooperation and CERT engagement.[207] In terms of cyber policy, a state with strong cyber maturity delivers well-resourced policy which focuses on CIP as well as engagement with the private and educational sectors.[208] A key factor in establishing cyber defence responsibility is inter-agency cooperation and information sharing between various agencies responsible for cyber defence.[209]

US AND ACCURATE THREAT ANALYSIS

The aim of this section is to evaluate the current US cyber threat challenges. America's current threat analysis focuses on the threats posed by state-based cyberespionage or cyberattacks on US interests above non-state cyberattacks and online recruitment by terrorist organisations.[210]

A growing challenge for the US and other western states will to defend against the threat of soft power state-based campaigns to undermine democratic confidence and potentially swing election results through the leaking and dissemination of sensitive information, which potentially has been accessed through hacking.[211] A major state-based cyberattack on the US in recent years was the hack of the Democratic National Convention (DNC) in July 2016 where over 19,000 politically sensitive emails and 8,000 attachments were leaked and

[206] W. Marmon, 'Main cyber threats now coming from governments as "state actors"', *The European Institute*, November 2011, https://www.europeaninstitute.org/index.php/136-european-affairs/ea-november-2011/1464-main-cyber-threats-now-coming-from-governments-as-state-actors, accessed 10 March 2017.

[207] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2016, *Australian Strategic Policy Institute*, 2016, pp. 6-9.

[208] G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security*, May 2016, pp. 13-20.

[209] K.M. Finklea, 'The Interplay of Borders, Turf, Cyberspace and Jurisdiction: Issues Confronting U.S. Law Enforcement', *Congressional Research Service*, 17 January 2013, pp. 25-34.

[210] L. Gribbon, V. Horvath, K. Robertson, N. Robinson, 'Cyber-security Threat Characterisation: A Rapid Comparative Analysis', RAND Corporation, 2013, pp. 28-30.

[211] J. Bund, 'Cybersecurity and Democracy: Hacking, Leaking and Voting', European Union Institute for Security Studies, Brief Issue, No. 30, November 2016, pp. 1-4.

published on WikiLeaks.[212] It is alleged by US intelligence officials that the hack was carried out by the Russian government in an effort to interfere with the election process and to undermine US democracy.[213] Despite Russia denying responsibility for the hack, this event indicates the high prioritization for defending against state-based or sponsored cyberattacks for the US government.[214] After the alleged interference with the US election, there is concern that Russia will attempt to apply these tactics to spread disinformation and effect upcoming elections in Europe in 2017.[215]

Another example of the high prioritization of state-based cyberattacks by the US was the 2014 Sony Pictures cyberattack.[216] The cyberattack came as a result of a hacker group named "The Guardians of Peace" leaking confidential data from Sony Pictures which contained sensitive information regarding the film studios.[217] After investigating the cyberattack, US intelligence such as the National Security Agency (NSA) and Federal Bureau of Investigation (FBI) alongside White House officials concluded that the North Korean government was "centrally involved" in the cyberattack.[218] This illustrates the high threat level for the US associated with attacks perpetrated by state-based actors on US targets.[219]

[212] S. Ackerman, S. Thielman, 'US officially accuses Russia of hacking DNC and interfering with election', in *The Guardian*, 9 October 2016, https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election, accessed 15 December 2016.

[213] Office of the Director of National Intelligence, 'Assessing Russian Activities and Intentions in Recent US Elections', *Intelligence Community Assessment*, 6 January 2017, pp. i-iii.

[214] T. Timm, 'The rush to blame Russia for the DNC email hack is premature', in *The Guardian*, 26 July 2016, https://www.theguardian.com/commentisfree/2016/jul/25/russia-blame-dnc-email-hack-premature, accessed 15 December 2016.

[215] D.M. Herszenhorn, 'Europe braces for Russia hacking in upcoming elections' *Politico*, 13 December 2016, http://www.politico.eu/article/europe-russia-hacking-elections/, accessed 19 February 2017.

[216] J.A. Lewis, 'Sony and North Korea: Making the Case', *Center for Strategic and International Studies*, 5 December 2014, https://www.csis.org/analysis/sony-and-north-korea-making-case, accessed 16 December 2016.

[217] *Ibid.*

[218] N. Perlroth, D.E. Sanger, 'US Said to Find North Korea Ordered Cyberattack on Sony' in *New York Times*, 17 December 2014, https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html, accessed 16 December 2016.

[219] B.W. Bennett, 'Did North Korea Hack Sony?', in *Rand Corporation*, 11 Decembr 2014, http://www.rand.org/blog/2014/12/did-north-korea-hack-sony-pictures-entertainment.html, 16 December 2016.

In contrast to the high prioritization of state-based cyberattacks, non-state cyberterrorism remains a secondary priority for the US government.[220] Whilst the US government has raised a high degree of alarm regarding the threat of non-state cyberterrorism, it has faced considerably fewer threats from non-state actors.[221] In 2015, Islamic state supporters hacked the US Central Command Twitter account and posted messages threatening US military personnel as well as pro-IS propaganda. An unsophisticated cyberattack such as this can be considered more embarrassing for the US government then being indicative of a major cyberattack against US critical infrastructure.[222] However, the threat of non-state groups attempting to launch sophisticated cyberattacks remains, In 2015 US officials reported that IS hackers had attempted and failed to penetrate computers which regulate the nation's electricity grid, a vital part of US critical infrastructure which indicates their current lack of cyber capabilities.[223] US threat analysis indicates that cyberterrorist groups such as IS' cyber programs are currently under resourced and lack enough technological capabilities to successfully commit cyberattacks on US critical infrastructure.[224]

The main challenge for the US is the ability to be transparent with the public regarding the risk of cyber threats without causing unnecessary alarm. To date, he US government has been

[220] G. Weimann, 'Cyberterrorism: How Real is The Threat?', *United States Institute of Peace*, December 2004, https://www.usip.org/sites/default/files/sr119.pdf, accessed 4 September 2016, pp. 8-10.

[221] F.J. Cilluffo, 'Testimony on Emerging Cyber Threats to the United States before the US House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Securities Technology', 2016, http://docs.house.gov/meetings/HM/HM08/20160225/104505/HHRG-114-HM08-Wstate-CilluffoF-20160225.pdf, accessed 10 December 2016, pp. 1-11.

[222] R. Berman, 'The Hacking of Central Command', *The Atlantic*, 12 January 2015, https://www.theatlantic.com/politics/archive/2015/01/central-command-accounts-are-hacked-centcom-isis-soldiers-obama-cybersecurity-cybercaliphate/384442/, accessed 18 December 2016.

[223] J. Marks, 'ISIL aims to launch cyberattacks on US', *Politico*, 29 December 2015, http://www.politico.com/story/2015/12/isil-terrorism-cyber-attacks-217179, accessed 18 December 2016.

[224]P.W. Singer, 'The Cyber Terror Boogeyman', *Brookings Institution*, 1 November 2012, https://www.brookings.edu/articles/the-cyber-terror-bogeyman/, accessed 10 September 2016.

unrestrained in cautioning the public about the threat associated with cyberterrorism.[225] In 2016, President Obama stated that foreign cyber threats:

> Continue to pose an unusual and extraordinary threat to the national security, foreign policy and economy of the United States.[226]

Language such as this indicates that the US is approaching public messaging regarding cyber threats by not underestimating the potential risks. Its challenge lies in its ability to not cause unnecessary alarm or panic.[227]

US AND COORDINATED INSTITUTIONAL STRUCTURE

The following section analyses the coordination of institutional structure reveals a whole-of-government approach to cyber governance.[228] Furthermore, US institutional cyber structure is positioned for strong cyber maturity due to its commitment to CERT engagement and international cooperation.[229]

Given its massive pool of resources, Carlin argues the US government has been able to construct an inter-connected whole-of government approach which aims to integrate intelligence, law enforcement and military agencies as well as strengthening the cybersecurity of all branches of the federal and state government.[230] At the core of the federal organisational structure of US cybersecurity is the National Security Council's Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC). The ICI-IPC is co-chaired by the Homeland Security Council and Cyber Security Coordinator (CSC) which

[225] G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center for Cyber Security*, May 2016, pp. 7-8.
[226] *Ibid.*
[227] P.W. Singer, 'The Cyber Terror Boogeyman', *Brookings Institution*, 1 November 2012, https://www.brookings.edu/articles/the-cyber-terror-bogeyman/, accessed 10 September 2016
[228] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2016', *Australian Strategic Policy Institute*, 2016, p. 83.
[229] *Ibid.*
[230] J.P. Carlin, 'Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats', in *Harvard National Security Journal*, Vol. 7, 2016, pp. 393-398.

has an extremely influential role in American cybersecurity.[231] The role of CSC, which is often referred to as "Cyber Czar,"[232] takes on the responsibility of the special assistant to the President on matters of cybersecurity as leading and overseeing the interagency development of national cybersecurity strategy and policy, as well as overseeing respective agencies' implementation of these policies.[233] The most important agencies that undertake cyber responsibility are a mixture of intelligence, law enforcement and military departments which embody the whole-of-government approach.[234] Some of these agencies include:

- Department of Homeland Security (DHS)[235]
- Office of Cyber Security and Communications (CS&C)[236]
- NSA[237]
- FBI[238]
- Central Intelligence Agency (CIA)[239]
- DOD[240]
- USCYBERCOM[241]
- Department of State (DOS)[242]

[231] P. Pernik, J. Wojtkowiak, A. Verschoor-Kirss, 'NATO Cyber Security Organisation: United States', *NATO Cooperative Defence Centre of Excellence*, pp. 15-16,

[232] T. Feakin, P. Jennings, 'The Emerging Agenda for Cybersecurity', *Australian Strategic Policy Institute*, July 2013, p. 4.

[233] *Ibid.*

[234] J.P. Carlin, 'Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats', in *Harvard National Security Journal*, Vol. 7, 2016, pp. 393-396.

[235] Department of Homeland Security, 'Cybersecurity', 27 September 2016, https://www.dhs.gov/topic/cybersecurity, accessed 20 December 2016.

[236] Department of Homeland Security, 'Office of Cybersecurity and Communications', 6 October 2016, https://www.dhs.gov/office-cybersecurity-and-communications, accessed 20 December 2016.

[237] National Security Agency, 'What we do: Cyber', 3 May 2016, https://www.nsa.gov/what-we-do/cyber/, accessed 20 December 2016.

[238] Federal Bureau of Investigation, 'What we investigate: Cyber Crime', 2016, https://www.fbi.gov/investigate/cyber, accessed 20 December 2016.

[239] G. Miller, 'CIA plans major reorganization and a focus on digital espionage', *Washington Post,* 6 March 2015, https://www.washingtonpost.com/world/national-security/cia-plans-major-reorganization-and-a-focus-on-digital-espionage/2015/03/06/87e94a1e-c2aa-11e4-9ec2-b418f57a4a99_story.html?utm_term=.d82ff692a6c0, accessed 20 December 2016.

[240] Department of Defense, 'The Department of Defense Cyber Strategy', 2015, pp. 1-9.

[241] *Ibid*, pp. 6-7.

- United States Computer Readiness Team (US-CERT)[243]
- Department of Justice (DOJ)[244]
- Cyber Threat Intelligence Integration Center (CIIT)[245]

The US government has focused on CIP with the establishment of US-CERT as its national computer readiness branch which is streamlined from within the DHS.[246] Although being vast in organisational structure, the 2016 ASPI Cyber Maturity Report graded the US' organisational structures as a 10 due to its ability to refine its governance of cyber issues and carefully clarify the roles and responsibilities of its agencies in cybersecurity incident responses for the public and private sectors.[247]

As identified in Chapter One, international engagement is essential in attaining cyber maturity.[248] The US can be viewed as one of the international leaders in engaging the global community on cybersecurity.[249] The US provides significant assistance to international partners to fight cyberattacks and cybercrime whilst taking part bilateral and multilateral regional forums, agreements and treaties aimed to enhance cyber norms in the global community.[250] The US has attempted to create a global counter narrative to what they consider to be the Chinese and Russian-led conception of international cyber policy and governance which has been characterized by allegations of state-based cyberattacks,

[242] US Department of State, 'Department of State International Cyberspace Policy Strategy', March 2016, pp. 1-12.
[243] United States Computer Readiness Team, 'About Us', 2016, https://www.us-cert.gov/about-us, accessed 20 December 2016.
[244] US Department of Justice, 'Cybersecurity Unit', 21 November 2016, https://www.justice.gov/criminal-ccips/cybersecurity-unit, accessed 20 December 2016.
[245] Office of the Director of National Intelligence, 'Cyber Threat Intelligence Integration Center: Who we are', 2015, https://www.dni.gov/index.php/about/organization/ctiic-who-we-are, accessed 20 December 2016.
[246] United States Computer Readiness Team, 'About Us', 2016, https://www.us-cert.gov/about-us, accessed 20 December 2016.
[247] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2016', *Australian Strategic Policy Institute*, 2016, p. 83.
[248] *Ibid*, p. 7.
[249] *Ibid*, p. 83.
[250] *Ibid.*

malicious cyber threats and internet censorship. The goal of the US counter narrative is one to promote an open, collaborative multistakeholder model of cyberspace.[251]

Alongside its cyber cooperation with Australia through treaties such as Five Eyes,[252] ANZUS[253] and the AUS-US Cyber Security Dialogue,[254] the US has aimed to strengthen ties with other allied states in cyber relations, developing bilateral plans for cyber-cooperation with Canada,[255] the UK,[256] Japan,[257] India,[258] South Korea,[259] EU states[260] as well as attempting to mend tense cyber cooperation with China.[261] On top of this the US has committed to international forums aiming to strengthen cyber norms such as the G20, ASEAN, the Organization for Security and Co-operation in Europe (OSCE)[262] as well as sponsoring the NATO Cooperative Cyber Defence Centre of Excellence.[263] These efforts for international engagement on cybersecurity by the US shows their commitment to leading the

[251] *Ibid.*

[252] G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center for Cyber Security*, May 2016, p.4.

[253] A. Davies, J. Herrera-Flanigan, L. Khalil, J. Lewis, J. Mulvenon, ‘ANZUS 2.0: Cybersecurity and Australia-US relations’, *Australian Strategic Policy Institute*, April 2016, Issue 46, pp. 1-3.

[254] Office of the Press Secretary, ‘Fact Sheet: United States – Australia Cooperation: Deepening our Strategic Partnership’, 19 January 2016, https://www.whitehouse.gov/the-press-office/2016/01/19/fact-sheet-united-states-%E2%80%93-australia-cooperation-deepening-our-strategic, accessed 21 December 2016.

[255] Public Safety Canada, ‘Cybersecurity Action Plan between Public Safety Canada and the Department of Homeland Security’, 2 December 2015, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-en.aspx, accessed 21 December 2016.

[256] Office of the Press Secretary, ‘Fact Sheet: US – United Kingdom Cybersecurity Cooperation, 16 January 2015, https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation, accessed 21 December 2016.

[257] US Department of State, ‘The 4th US-Japan Bilateral Cyber Dialogue’, 27 July 2016, https://www.state.gov/r/pa/prs/ps/2016/07/260572.htm, accessed 21 December 2016.

[258] Office of the Press Secretary, ‘Joint Statement: 2015 United States-India Cyber Dialogue’, 29 September 2016, https://www.whitehouse.gov/the-press-office/2016/09/29/joint-statement-2016-united-states-india-cyber-dialogue, accessed 21 December 2016.

[259] Office of the Press Secretary, ‘Joint Fact Sheet: The United States – Republic of Korea Alliance: Shared Values, New Frontiers’, 16 October 2015, https://www.whitehouse.gov/the-press-office/2015/10/16/joint-fact-sheet-united-states-republic-korea-alliance-shared-values-new, accessed 21 December 2016.

[260] Office of the Press Secretary, ‘Fact Sheet: US – EU Cyber Cooperation’, 26 March 2014, https://www.whitehouse.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation, accessed 21 December 2016.

[261] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2016', *Australian Strategic Policy Institute*, 2016, p. 83.

[262] *Ibid.*

[263] NATO Cooperative Cyber Defence Centre of Excellence, ‘About Cyber Defence Centre’, 2016, https://ccdcoe.org/about-us.html, accessed 21 December 2016.

way in the global community in promoting the cyber norms of a free and open internet, developing strong cybersecurity and opposing cybercrime.[264]

US AND COHERENT CYBER POLICY

Current US cyber policy is consistent with the research provided in Chapter One which underscores the importance of cyber policy which prioritizes CIP[265] through a well-funded national strategy [266] which also focuses on cyber education [267] and private sector engagement.[268] Announced in 2016, the Cybersecurity National Action Plan (CNAP) was the Obama Administration's cornerstone cybersecurity policy platform.[269] The goal of CNAP was to build upon the work made of the Cyber Information Sharing Act of 2015; legislation that passed through Congress which was designed to allow for stronger cybersecurity in the US through enhanced sharing regarding cybersecurity threats between the US government and the private sector.[270] CNAP aimed to build upon that by creating a comprehensive national cybersecurity strategy for the short and long term which is designed to enhance cybersecurity protections and awareness, protect privacy, and maintain public safety as well as economic and national security.[271] The key issues and directives which the Obama administration aimed to address within this executive order are outlined in Figure 3.1:

[264] US Department of State, 'Department of State International Cyberspace Policy Strategy', March 2016, pp. 1-12.

[265] A. MacGibbon, 'Cyber Security: Threats and Responses in the Information Age', *Australian Strategic Policy Institute*, December 2009, Issue 26, p. 10.

[266] A. Ariely, 'Adaptive Responses to Cyberterrorism', Cyberterrorism: Understanding, Assessment, and Response, Springer Publishing, 2014, pp. 180-181.

[267] G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security*, May 2016, pp. 16-20.

[268] T. Feakin, P. Jennings, 'The Emerging Agenda for Cybersecurity', *Australian Strategic Policy Institute,* July 2013, p. 9.

[269] Office of the Press Secretary, 'Fact Sheet: Cybersecurity National Action Plan', 9 February 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan, accessed 24 December 2016.

[270] *Ibid.*

[271] *Ibid.*

Figure 3.1: W2 Communications Fact Sheet: Cybersecurity National Action Plan

Figure removed due to copyright restriction

Source: W2 Communications, ‘Fact Sheet – Cyber Security National Action Plan’, February 2016, https://www.w2comm.com/fact-sheet-cybersecurity-national-action-plan/, accessed 24 December 2016.

NCAP had a strong focus on CIP as exemplified by the $3.1B IT Modernization Fund.[272] The goal of the modernization fund is retiring, replacing and modernizing antiquated IT infrastructure, networks and systems within the US.[273] Furthermore, CNAP aimed to improve

[272] *Ibid.*

[273] *Ibid.*

CIP by establishing the National Center for Cybersecurity Resilience where public and private organisations can test the security of their systems in a contained environment.[274]

A vital part of CNAP is the Commission on Enhancing National Cybersecurity as it encourages private sector engagement, essential for coherent cyber policy.[275] This Commission will be designed with the objective of bringing together bi-partisan Congressional leadership, federal and state leadership as well as leaders from the private sector to bolster strong relationships and collaboration amongst a variety of experts from numerous fields.[276] The goal of the Commission is to make recommendations on the future of American cybersecurity with the goal of strengthening the public and private sector's cyber infrastructure through mutual collaboration between these various experts.

Through CNAP, the Obama Administration made a commitment to cyber education by investing in various programs aimed at improving the number of experts, skilled-workers and academic institutions committed to advancing US cybersecurity.[277] The CNAP is illustrative of the US taking the right steps to further its strong cyber maturity with a commitment to cyber education, a major component of coherent cyber policy. CNAP has attempted to improve US cyber education with the inclusion of The CyberCorps Reserve Program, the Cybersecurity Core Curriculum and the National Centers for Academic Excellence in Cybersecurity program.[278] Alongside these policy plans, a cornerstone of recent federal government-driven cyber education efforts the National Initiative for Cybersecurity Careers and Studies (NICCS)[279]. NICCS stems from the DHS, through working with other government agencies, NICCS aim to utilize a whole-of-government approach as well as

[274] *Ibid.*
[275] *Ibid.*
[276] *Ibid.*
[277] *Ibid.*
[278] *Ibid.*
[279] Department of Homeland Security, 'DHS Launches National Initiative for Cybersecurity Careers and Studies', 21 February 2013, https://www.dhs.gov/news/2013/02/21/dhs-launches-national-initiative-cybersecurity-careers-and-studies, accessed 27 December 2016.

collaboration with the private sector aimed at improving cyber education within the US and developing the next generation of skilled cybersecurity workers.[280] Government efforts such as NICCS is an example of the US government striving towards strong cyber education within its workforce and education system which is essential for strong cyber maturity.[281]

An essential component of coherent cyber policy is the commitment to dedicate significant resources to cyber governance. As part of CNAP, the Obama Administration had allocated $19 billion USD of its fiscal year budget of 2017 which is a 35 per cent increase from its 2016 budget allocation to cybersecurity of $14 million USD.[282] The US efforts to make sizeable budgetary commitments towards cybersecurity has only increased their strong cyber maturity.[283]

One of the major challenges for US cyber policy in recent years has been that of the Washington political gridlock which has slowed down the passage of cyber policy. As of 2016, there were close to 30 bills under consideration in both houses. Disagreement within Congress has led to cyber legislation being delayed for several years, particularly as it pertains to the issue of encryption.[284] As well as causing gridlock in Congress, the issue of encryption has caused tension between the government and the private sector which will prove to be a challenge for US cyber policy in the future.[285] The 2016 legal dispute between Apple and the FBI over unlocking the cryptographically protected cell phone of the San Bernardino shooter is one example of the potential challenges between the government and

[280] *Ibid.*

[281] G. Austin, J. Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center for Cyber Security*, May 2016, pp. 16-20.

[282] *Ibid.*

[283] G. Austin, 'Australia still doesn't see a cyber attack as the menace our allies fear', *The Conversation*, April 25 2016, https://theconversation.com/australia-still-doesnt-see-a-cyber-attack-as-the-menace-our-allies-fear-57719, accessed 10 November 2016.

[284] Australian Strategic Policy Institute, 'Cyber *Maturity* in the Asia-Pacific Region 2016', *Australian Strategic Policy Institute*, 2016, pp. 81-83

[285] *Ibid.*

the private sector. This issue is likely to prove problematic to the health of public-private sector cooperation in the future.[286]

US AND ESTABLISHMENT OF CYBER DEFENCE RESPONSIBILITY

The culture of largely shared responsibility which exists between US intelligence agencies emphasizes inter-agency cooperation and information sharing.[287] The seemingly vast and endless organisational structure of American cyber institutions as pictured in Figure 3.2 has created a cyber culture where the burden of cybersecurity does not rest solely on one department or agency.[288]

[286] D. Yadron, 'US efforts to regulate encryption have been flawed, government reports find', *The Guardian,* 30 June 2016, https://www.theguardian.com/technology/2016/jun/29/government-encryption-regulation-report-criticism, accessed 24 December 2016.

[287] J.P. Carlin, 'Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats', in *Harvard National Security Journal,* Vol. 7, 2016, pp. 393-398.

[288] *Ibid.*

Figure 3.2: Schematic Diagram of Federal Agency Cybersecurity Roles.

Figure removed due to copyright restriction

Source: Fischer, E.A., 'Cybersecurity Issues and Challenges: In Brief', *Congressional Research Service*, 12 August 2016, p. 4.

The responsibility of protecting cybersecurity has largely fallen under the jurisdiction of the US Intelligence Community (IC)[289] as well as the DOD.[290] The 16 government agencies which fall under the IC, as well as DOD agencies such as USCYBERCOM, can be understood as having a balance of both unilateral and shared responsibility and jurisdiction

[289] E.A. Fischer, 'Cybersecurity Issues and Challenges: In Brief', *Congressional Research Service*, 12 August 2016, pp. 3-4.

[290] US Department of State, 'Department of State International Cyberspace Policy Strategy', March 2016, pp. 1-12.

with other IC agencies to respond to cyber threats and maintain US cybersecurity.[291] The IC has attempted to build an organisational culture which is committed to inter-agency cooperation and information sharing through the use of joint task forces and fusion centres such as the National Cyber Investigative Joint Task Force.[292] Furthermore, these intelligence agencies have higher policing capabilities which suit them best as they operate within the secretive space of national security.[293] Within the IC, the NSA has had an increased role within the task of maintaining US cybersecurity in recent years. This is due in part to its role in global surveillance programs as well as their role in cyber defence as having joint control over USCYBERCOM with the DOD.[294] This illustrates the joint responsibility and whole-of-government approach within the IC in maintaining US cybersecurity.[295] Outside of the formal structure of the IC, the DHS has significant cybersecurity responsibility and is pivotal to US cyber protection.[296] As the DHS responsibility to protect and maintain US national security has expanded since 9/11, so too has its responsibility to maintain and protect US cybersecurity and oversee CIP as well as cooperating with the IC through inter-agency cooperation and information sharing.[297]

The major US challenges lie in reducing competition and disagreement within the IC over cybersecurity responsibility. Although USCYBERCOM is under dual NSA and DOD

[291] J.P. Carlin, 'Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats', in *Harvard National Security Journal*, Vol. 7, 2016, pp. 393-398.

[292] C. Uhoff, 'Strategic Cyber Intelligence: An Examination of Practices across Industry, Government and Military', Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practise, Palgrave Macmillan, 2015, pp. 205-2015.

[293] B. Akhgar, F. Bosco, A. Staniforth, Cyber Crime and Cyber Terrorism Investigator's Handbook, Syngress, pp. 40-41.

[294] A. Davies, 'Cyber Wrap Special: two heads are better than one', *Australian Strategic Policy Institute*, 21 September 2016, https://www.aspistrategist.org.au/cyber-wrap-special-two-heads-better-one/, accessed 28 December 2016.

[295] *Ibid.*

[296] J. Holl Lute, 'Testimony on DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure to the US House of Representatives Committee on Homeland Security, 13 March 2013, file://usergh/h/hold0085/Downloads/nps59-032913-02%20(2).pdf, pp. 1-10.

[297] R. Perl, 'The Department of Homeland Security: Background and Challenges', Terrorism: Reducing Vulnerabilities and Improving Responses: US – Russia Workshop Proceedings, National Academies Press, 2004, pp. 176-178.

leadership, here have been calls within the IC and the Pentagon to break up the split-leadership structure.[298] This is due to the belief that the two departments have fundamentally different missions, one being focused on cyber espionage and the other being cyberwarfare and that both parties should not compete to use the same networks.[299] The calls for the leadership split reflects a growing debate over how to organize cyber military operations as they become more distinct and move away from the intelligence community. Both parties support the split in order to avoid a culture of competition within the bedrock of US cybersecurity capabilities.[300]

A culture of competition has led to agencies responsible for cybersecurity feuding with one another over cyber primacy. Tension between agencies has come as a result of the differing opinions over jurisdiction. Both departments want to take the lead on threat response. For instance, the Obama administration historically saw that it was the primary responsibility of the DHS, not the NSA to respond to these threats.[301] Another cause of tension is the differing intelligence assessments. A recent example of this was disagreement between the greater certainty of the CIA assessment *vis-a-vis* the FBI on the alleged motivations of Russian interference with the 2016 US election.[302] Furthermore, distrust between the intelligence communities over leaked information is proving to be a challenge. For instance, in 2010, a DoD official commented that:

[298] E. Nakashima, ‘Obama to be urged to split cyberwar command from NSA’, *Washington Post*, 13 September 2016, https://www.washingtonpost.com/world/national-security/obama-to-be-urged-to-split-cyberwar-command-from-the-nsa/2016/09/12/0ad09a22-788f-11e6-ac8e-cf8e0dd91dc7_story.html?utm_term=.e6dbb84132a3, accessed 23 December 2016.

[299] *Ibid.*

[300] *Ibid.*

[301] J. Emspak, ‘Feuding agencies agree to disagree on cybersecurity’, *NBC News*, 31 August 2011, http://www.nbcnews.com/id/44350731/ns/technology_and_science-security/t/feuding-agencies-agree-disagree-cybersecurity/#.WKjnwW-GPIU, accessed 23 September 2016.

[302] A. Entous, E. Nakashima, ‘Divisions between CIA, FBI surface in debate over Russian motives in election hack’, *Chicago Tribune*, 10 December 2016, http://www.chicagotribune.com/news/nationworld/politics/ct-russian-election-tampering-cia-fbi-20161210-story.html, accessed 19 February 2017.

> There is disagreement, particularly in the US intelligence community, as to whether the benefits of showing cyber-threat information outweigh the risk of harm to US security interests should sensitive data be leaked to an adversary of the US.[303]

These types of disagreements illustrate that self-interest and competition over jurisdiction and responsibility are a major factor in tension within the US cyber community.[304] A focus on developing stronger information sharing and inter-agency cooperation such as fusion centres and inter-agency task forces within the IC is necessary to address this challenge.[305]

Another challenge for the US will be balancing shared cyber responsibility with its rapid growth of cyber militarization. It is Wallace's belief that excessive growth in cyber militarization will create a heavy reliance on defence departments whereas he believes law enforcement agencies and the private sector should expand their role in cybersecurity.[306] Cyber capabilities of the US military appear to be expanding at a rapid rate. The USCYBERCOM 2018 goal is to reach its intended target of recruiting 6,200 troops for its 133 cyber teams within the recently established Cyber Mission Force teams.[307] The DoD budget for cyber defence spending for the FY 2017 is USD 6.7 billion which illustrates the rapid expansion and growth of the US militaries cyber capabilities.[308] Nevertheless, ASPI

[303] D. Clark, W. Diffie, A.D. Sofaer, 'Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy, National Academies Press, 2010, pp. 184-185.

[304] J. Emspak, 'Feuding agencies agree to disagree on cybersecurity', *NBC News*, 31 August 2011, http://www.nbcnews.com/id/44350731/ns/technology_and_science-security/t/feuding-agencies-agree-disagree-cybersecurity/#.WKjnwW-GPIU, accessed 23 September 2016.

[305] K.M. Finklea, 'The Interplay of Borders, Turf, Cyberspace and Jurisdiction: Issues Confronting U.S. Law Enforcement', *Congressional Research Service*, 17 January 2013, pp. 20-24.

[306] I. Wallace, 'The Military Role in National Cybersecurity Governance', *Brookings Institution*, 16 December 2013, https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/, accessed 23 September 2016.

[307] US Department of Defense, 'All Cyber Mission Force Teams Achieve Initial Operating Capability', *US Department of Defense*, 24 October 2016, https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability, accessed 9 April 2017.

[308] US Department of Defense, 'Fiscal Year 2017 Budget Fact Sheet', 2016, https://www.defense.gov/Portals/1/features/2016/0216_budget/docs/2-4-16_Consolidated_DoD_FY17_Budget_Fact_Sheet.pdf, accessed 28 December 2016. p 5.

rates US military cyber capabilities as a 10.[309] Significant growth in cyber militarization is also to be expected from a great power such as the US who will continue to compete with rivals such Russia, China, and Iran.[310] This future challenge will be in the maintenance of its cyber defence responsibility as the DoD's role begins to grow exponentially.[311]

CONCLUSION

US cyber infrastructure and capabilities are amongst the strongest in the world. Based on its vulnerability and targeting by state-based cyber threats, the US has evaluated these threats as higher than non-state threats due to the higher risk of damage they pose to critical infrastructure. Within its cyber institutions, the US has created a vast, widespread whole-of-government infrastructure which is designed to create cooperation between various agencies and departments which stem from intelligence, law enforcement and defence. Its commitment to engaging international allies in cyber cooperation is further indicative of strong cyber maturity. A criticism of the vastness of their cyber institutions is that it can result in competition and disagreement. Nonetheless, the Obama Administration created a well-resourced national cyber policy which focused on investing in CIP and national cyber education as well as engagement with the private sector. The militarization of US cybersecurity seems to be growing rapidly which follows a trend in global cybersecurity in becoming militarized. Overall, the US is one of the global trendsetters and has extremely strong cyber maturity based on its institutions, policy, resources, size and scope. Its position as a great power in the international community has led it to becoming a major target for state

[309] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2016', *Australian Strategic Policy Institute*, 2016, p. 83.

[310] US Department of Defense, 'The DoD Cyber Strategy', April 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, accessed 28 December 2016, p. 5; I. Wallace, 'The Military Role in National Cybersecurity Governance', *Brookings Institution*, 16 December 2013, https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/, accessed 23 September 2016.

[311] US Department of Defense, 'Fiscal Year 2017 Budget Fact Sheet', 2016, https://www.defense.gov/Portals/1/features/2016/0216_budget/docs/2-4-16_Consolidated_DoD_FY17_Budget_Fact_Sheet.pdf, accessed 28 December 2016. p 5.

and non-state based cyberattacks but its strong cyber maturity leaves it well positioned to protect US interests and defend against these threats.

CHAPTER FOUR:
Evolving Alliance: the Argument for Australia-US Cyber Cooperation

INTRODUCTION

The aim of this chapter is to provide evidence and recommendations as to why Australia and the US should deepen their cyber cooperation to both strengthen their strategic alliance and cyber maturity: all of which will in turn fortify their national security interests. By examining the growth in cyber cooperation as seen in institutions of strategic engagement such as ANZUS, the US-Australia Cyber Dialogue and Five Eyes, this chapter will illustrate that a healthy cyber relationship is beneficial to both states. It is argued that cyber cooperation between both states is essential for cyber maturity. International engagement is said to improve cyber maturity because it builds greater cooperation, transparency, stronger security alliances as well as promoting international norms and laws advocating for a free and open internet and malicious cyber threat deterrence.[312] Cyber cooperation between Australia and the US deepens their historic strategic alliance through expanded information sharing, coordinated technological investment as well as strengthening a commitment to fighting cybercrime.[313] Furthermore, this chapter argues that cyber maturity is achieved through cooperative expansion of private sector engagement by both states and through a shared commitment to reinforcing cyber norms such as a free and open internet and malicious threat deterrence.

As is the case with the current state of the alliance, a potential hurdle to cyber cooperation is the juxtaposition of Australia's long-standing trade relationship with China and its strategic alliance with the US. Australia must carefully balance its relations with both states due to the

[312] M. Hasan, 'International Cyber Security Cooperation', *Modern Diplomacy*, 13 November 2016, http://moderndiplomacy.eu/index.php?option=com_k2&view=item&id=1894:international-cyber-security-cooperation&Itemid=154, accessed 18 January 2017.

[313] D. Nichola, 'Expanding Alliance: ANZUS Cooperation and Asia-Pacific security', *Australian Strategic Policy Institute*, December 2014, p. 21.

high potential for disagreement and animosity between China and the US on cyber policy in the foreseeable future.[314] Special consideration should be given too, to the challenge of maintaining consistent messaging in cyber policy between both states as the Trump Administration takes office.[315]

INTERNATIONAL COOPERATION AS KEY TO CYBER MATURITY: THE CASE FOR THE AUSTRALIA-US ALLIANCE

As argued in Chapter One, a key factor in attaining cyber maturity is for states to engage in international cooperation with regional and global partners. International cooperation is viewed as beneficial to cyber maturity because it promotes stronger security alliances, open and transparent communication regarding cybersecurity, a strong global cyber community infrastructure and protects mutual economic and national security interests.[316]

Alongside this, international cooperation is beneficial is because it aims to promote international norms and laws which encourage a free and open internet and malicious cyber threat deterrence and responses.[317] International cyber cooperation is necessary for national security as it establishes norms of appropriate activities in cyberspace, develops standards for state responsibility for cyberattacks launched within a state's territory, and for identifying practices for deterring and defending against non-state cyberterrorists.[318] Some of the most common forms of international cyber cooperation include bilateral and multilateral cyber

[314] K. Lieberthal, P.W. Singer, 'Cybersecurity and U.S.-China Relations', *Brookings Institution,* February 2012, pp. 2-6.

[315] R. Medcalf, M. Sussex, M. Tsirbas, R. Young, 'The Trump Presidency and Australia's security: don't panic, don't relax', *National Security College (ANU),* Policy Options Paper, No. 1, January 2017, p. 2.

[316] G. Waters, 'The Case for a Regional Cyber Security Action Task Force', *Institute for Regional Security,* Security Challenges, Vol. 7, No. 1, Autumn 2011, p. 4.

[317] Information Security Policy Council (Japan), 'International Strategy on Cybersecurity Cooperation: J-initiative for Cybersecurity', *National Center of Incident Readiness and Strategy for Cybersecurity,* 2 October 2013, pp. 1-2.

[318] A.M. Wolf, A. Litchman, 'Workshop Summary Report: Cyber Threats and International Cooperation', *Council on Foreign Relations,* February 2015, pp. 1-3.

agreements, security treaties and alliances, international cyber legal frameworks, as well as diplomatic dialogues on cybersecurity.[319]

Based on their strong strategic alliance predicated on shared cultural values, interests and norms, Australia and the US are well positioned to enhance their cyber cooperation, which would result in stronger cyber maturity for both states. Both states share a historical strategic alliance, which can be traced back to the signing of the ANZUS Treaty in 1951, and has been characterized by strong coordinated military efforts between these states in both World Wars as well as conflicts in Korea, Vietnam, Iraq and Afghanistan.[320]

Currently, Australia’s geopolitical positioning is viewed as key to the US rebalance to Asia strategy. The US is of key strategic value to Australia as its military and political power and strength brings a sense of security and stability to Australia’s strategic outlook in the Asia-Pacific.[321] The alliance can be viewed as being of mutual benefit to both states as they seek like-minded powers to maintain a balance of power and promote existing rules and norms within the Asia-Pacific.[322] Australia has traditionally purchased the majority of its major weapons systems from the US. Most recently it includes the purchase of the Lockheed Martin F-35A Joint Strike Fighter. In terms of recent military cooperation, Australia and the US have engaged with one another in in the global coalition to halt the growth of Islamic State troops in Iraq and Syria.[323]

[319] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2016', *Australian Strategic Policy Institute*, 2016, p. 7.

[320] T. Lum, B. Vaughn, ‘Australia: Background and U.S. Relations’, *Congressional Research Service*, 14 December 2015, https://fas.org/sgp/crs/row/RL33010.pdf, accessed 20 January 2017, p. I.

[321] *Ibid.*

[322] R. Fontaine, ‘Against Complacency: Risks and Opportunities for the Australia-US Alliance’, *United States Studies Centre*, p. 4.

[323] T. Lum, B. Vaughn, ‘Australia: Background and U.S. Relations’, *Congressional Research Service*, 14 December 2015, https://fas.org/sgp/crs/row/RL33010.pdf, accessed 20 January 2017, pp. 1-2.

Additionally, in 2014 the US announced it would increase marines through Darwin to a full contingent of 2500 troops by 2017.[324] Alongside the plans for troop rotations in Darwin, the Joint Posture Agreement laid the groundwork for alliance defence initiatives, such as ballistic missile defence and trilateral military exercises within South East Asia.[325] On top of these measures to deepen the strategic and military relationship, Australia and the US were working towards deepening bilateral cooperation in the areas of cyber defence and cyber security incident response.[326]

Cyber cooperation has expanded immensely since the September 11 attacks, while increased cooperation in intelligence gathering was created in part by the security needs arising from the 'War on Terror'. Intelligence gathering cooperation can be traced back to the ANZUS Treaty activation in 2001 and the 2004 removal of the No Foreign Access restriction on the US SIPRINET interconnected computer network system, allowing cooperation between the two states.[327] There has since been a direct effort to engage with one another on cybersecurity based on their long-standing alliance, current strategic interests and to increase the cyber maturity of their own state's cybersecurity infrastructure. Mutual shared values between both states include an open, interoperable, secure and reliable internet, which also protects the privacy of their citizens.[328] It is in both states' mutual interests to cooperate on cybersecurity by promoting peacetime norms for cyber and mapping out cooperative cyber incident

[324] J. Brown, 'Australia-US Defence Deal: What it means', *The Lowy Institute,* 13 June 2014, https://www.lowyinstitute.org/the-interpreter/australia-us-defence-deal-what-it-means, accessed 20 January 2017.
[325] *Ibid.*
[326] T. Lum, B. Vaughn, 'Australia: Background and U.S. Relations', *Congressional Research Service,* 14 December 2015, https://fas.org/sgp/crs/row/RL33010.pdf, accessed 20 January 2017, p. 2.
[327] M. Kelton, 'Arresting diffusion: Evolving spatial domains of power in the Australia-US alliance', Paper for the ISA Annual Convention, San Francisco, 3-6 April 2013, p. 10.
[328] Office of the Press Secretary, 'Fact Sheet: United States – Australia Cooperation: Deepening Our Strategic Partnership', January 19 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/01/19/fact-sheet-united-states-%E2%80%93-australia-cooperation-deepening-our-strategic, accessed 19 January 2017.

deterrents as well as response structures and mechanisms in the event of malicious cyber threats and cybercrime.[329]

Cyber cooperation is beneficial particularly from an Australian perspective due to a changing military balance in the Western Pacific; cyber cooperation allows Australia to pursue a new avenue with its closest strategic ally.[330] Deepening cyber cooperation with the US will allow Australia to pursue stronger relationships with US public and private sector partners,[331] whilst strengthening strategic interests through coordinated technological investment, expanded information sharing capabilities.[332] Furthermore, cyber cooperation will further strengthen the alliance by a further commitment to fight cybercrime in the Asia-Pacific collaboratively with the US.[333] There are a number of areas in which cyber cooperation between Australia and the US is already being engaged and stands to be deepened and improved upon. In terms of priorities, the most important institutions and areas of engagement of the alliance pertaining to cyber cooperation are 1.ANZUS 2. The Australia-US Cyber Dialogue, and finally 3. The Five Eyes Treaty.[334]

ANZUS

ANZUS is of the highest importance to alliance cyber cooperation because it provides the framework for how both states should coordinate with each other on cybersecurity. The ANZUS Treaty stands to serve as a basis for promoting norms regarding cyber threat

[329] ASPI International Cyber Policy Centre, 'ASPI and CSIS to bring together new Australia-US Cyber Dialogue', *Australian Strategic Policy Institute,* 20 January 2016, https://www.aspistrategist.org.au/aspi-and-csis-to-bring-together-new-australia-us-cyber-security-dialogue/, accessed 22 January 2017.

[330] D. Nichola, 'Expanding Alliance: ANZUS Cooperation and Asia-Pacific security', *Australian Strategic Policy Institute*, December 2014, p. 20.

[331] Z. Hawkins, 'The US-Australia Cyber Dialogue: cooperation in the Asia-Pacific', *Australian Strategic Policy Institute*, 1 November 2016, https://www.aspistrategist.org.au/us-australia-cyber-dialogue-cooperation-asia-pacific/, accessed 21 January 2017.

[332] D. Nichola, 'Expanding Alliance: ANZUS Cooperation and Asia-Pacific security', *Australian Strategic Policy Institute*, December 2014, pp. 20-21.

[333] Z. Hawkins, L. Nevill, 'The US-Australia Cyber Dialogue: fighting cybercrime in the Asia-Pacific', *Australian Strategic Policy Institute,* 4 November 2016, https://www.aspistrategist.org.au/us-australia-cyber-dialogue-fighting-cybercrime-asia-pacific/, accessed 23 January 2017.

[334] 'Cyber Maturity in the Asia-Pacific Region 2016', *Australian Strategic Policy Institute*, 2016, p. 7.

deterrent as well as establishing procedures with one another regarding how they should cooperate and respond in the event of a cyberattack on either party.[335] This is because the issue of cybersecurity was recognized in 2011 as a legal and collaborative dimension within the ANZUS treaty. The recognition of cybersecurity within the ANZUS Treaty is beneficial to Australia-US relations because it stands to strengthen the alliance as well as prioritizing cybersecurity as a national security issue for both states.[336] By recognizing cybersecurity as dimension within ANZUS it elevates cybersecurity as a priority cooperative effort alongside historically strong sectors of national defence such as maritime, land forces and air power.[337]

As part of the 2014 Australia-United States Ministerial Consultations (AUSMIN) it was announced that the treaty continues to act as a regional commitment to peace and security in the Asia-Pacific. Alongside this both parties stressed the legal and collaborative dimensions of ensuring cybersecurity, which fall under their ANZUS commitment.[338] The collaborative dimension both states shared with one another in relation to cybersecurity was initially explained at the 2011 AUSMIN joint statement that:

> In the event of a cyberattack that threatens the territorial integrity, political independence, and security of either of our nations, Australia and the US would consult together and determine appropriate options to address the threat.[339]

[335] C. Sullivan, 'Cybersecurity and the ANZUS treaty: The issue of U.S.-Australian Retaliation', *Georgetown Journal of International Affairs*, 27 August 2014, http://journal.georgetown.edu/cybersecurity-and-the-anzus-treaty-the-issue-of-u-s-australian-retaliation/, accessed 23 January 2017.

[336] *Ibid.*

[337] C. Sullivan, 'Cybersecurity and the ANZUS treaty: The issue of U.S.-Australian Retaliation', *Georgetown Journal of International Affairs*, 27 August 2014, http://journal.georgetown.edu/cybersecurity-and-the-anzus-treaty-the-issue-of-u-s-australian-retaliation/, accessed 23 January 2017.

[338] C. Sullivan, 'Cybersecurity and the ANZUS treaty: The issue of U.S.-Australian Retaliation', *Georgetown Journal of International Affairs*, 27 August 2014, http://journal.georgetown.edu/cybersecurity-and-the-anzus-treaty-the-issue-of-u-s-australian-retaliation/, accessed 23 January 2017.

[339] *Ibid.*

The requirement for cooperation in response to threats, which the ANZUS treaty obliges, illustrates why this treaty is well suited to facilitate cyber cooperation due to rising global concerns of malicious cyber threats.[340] By including cyber within the parameters of ANZUS, creates the opportunity for joint assessments of cyber threat, commonality of doctrine for offensive and defensive cyber operations, and cooperative delineation between cyber and electronic warfare capabilities.[341] In light of regional power and military balance shifts, such as increased force posture by China and North Korea within cyberspace, the recognition of cybersecurity as a collaborative dimension within the ANZUS treaty serves to advance both state's strategic and security interests within the Asia-Pacific.[342]

AUSTRALIA-US CYBER DIALOGUE

As the research in Chapter One suggested, diplomatic engagement between states is an essential part of attaining cyber maturity through international cooperation.[343] A recent example of this form of diplomatic engagement between Australia and the US is the newly established annual Australia-US Cyber Dialogue. It was announced in 2016 that both states would collaborate in an annual cyber dialogue beginning with its first inaugural session in September that year.[344] The goal of the initiative is guide the future direction of cyber policy in both states and to engage representatives and leaders from government and the private sectors by building collaborative cyber-capacity projects.[345] The cyber dialogue follows on

[340] *Ibid.*
[341] D. Nichola, 'Expanding Alliance: ANZUS Cooperation and Asia-Pacific security', *Australian Strategic Policy Institute*, December 2014, p. 21.
[342] A. Davies, P. Jennings, D. Nichola, B. Schreer, 'Expanding Alliance: ANZUS Cooperation and Asia-Pacific security', *Australian Strategic Policy Institute*, 2 December 2014, https://www.aspistrategist.org.au/expanding-alliance-anzus-cooperation-and-asia-pacific-security/, 20 February 2017.
[343] Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2016', *Australian Strategic Policy Institute*, 2016, p. 7.
[344] ASPI International Cyber Policy Centre, 'ASPI and CSIS to bring together new Australia-US Cyber Security Dialogue', *Australian Strategic Policy Institute*, 20 January 2016, https://www.aspistrategist.org.au/aspi-and-csis-to-bring-together-new-australia-us-cyber-security-dialogue/, accessed 21 January 2017.
[345] T. Feakin, 'The US-Australia Cyber Dialogue: prioritising cyber between strategic partners', *Australian Strategic Policy Institute,* 25 October 2016, https://www.aspistrategist.org.au/prioritising-cyber-strategic-partners-us-australia-cyber-dialogue/, accessed 23 January 2017.

from a recent formal commitment to cybersecurity discussion as part of the 2011AUSMIN dialogue, which laid the groundwork for diplomatic engagement between both states. [346]

As part of the cyber dialogue, both states aim to strengthen diplomatic engagement on cybersecurity by fortifying cyber cooperation in the Asia-Pacific and have plans to initiate dual-partnerships with the private sector within the region. This can result in cyber maturity to due to the opportunity for intelligence sharing capabilities of both states and the private sector as well as modernising international and cross-sectoral threat sharing mechanisms.[347] It is a necessity for both states to engage with the private sector in the Asia-Pacific to protect the business community from cybercrime, which in turn ensures the growth of stable, digital markets in the region, which protects their strategic and economic interests. An approach taken to enhance the capability of the private sector to protect itself from cyber threats is beneficial for both states.[348]

To defend against and weaken the threat of cybercrime Australia has agreed to enter an information-sharing framework with the DHS, which will strengthen a bilateral effort to remove cybercrime havens in the Asia-Pacific through threat information sharing. As the private sector is often a target of cybercrime, including information sharing agreements with the business community can only strengthen the public-private partnership for both states as well as protecting their economic security.[349] At the culmination of 2016's inaugural session, a work plan was agreed upon by which ASPI and CSIS will collaborate over a period of 12

[346] K. Rudd, 'Cooperation on Cyber – a new dimension of the US alliance', *Former Minister for Foreign Affairs: The Hon Kevin Rudd MP*, 15 September 2011, http://foreignminister.gov.au/releases/Pages/2011/kr_mr_110916.aspx?ministerid=2, accessed 21 January 2017.

[347] Z. Hawkins, 'The US-Australia Cyber Dialogue: cooperation in the Asia-Pacific', *Australian Strategic Policy Institute*, 1 November 2016, https://www.aspistrategist.org.au/us-australia-cyber-dialogue-cooperation-asia-pacific/, accessed 21 January 2017.

[348] T. Feakin, 'The US-Australia Cyber Dialogue: prioritising cyber between strategic partners', *Australian Strategic Policy Institute*, 25 October 2016, https://www.aspistrategist.org.au/prioritising-cyber-strategic-partners-us-australia-cyber-dialogue/, accessed 23 January 2017.

[349] Z. Hawkins, L. Nevill, 'The US-Australia Cyber Dialogue: fighting cybercrime in the Asia-Pacific', *Australian Strategic Policy Institute*, 4 November 2016, https://www.aspistrategist.org.au/us-australia-cyber-dialogue-fighting-cybercrime-asia-pacific/, accessed 23 January 2017.

months. Three focus areas were highlighted in the plan, which included programs to increase capacity-building efforts, undertaking a joint US-Australia led cyber exercise, and conducting research on how to overcome bilateral and regional barriers to trade.[350]

FIVE EYES

As aforementioned, strong cyber maturity can be achieved by robust information sharing between states. The Five Eyes intelligence alliance provides a unique opportunity for both states to improve their cyber cooperation through information sharing activities.[351] The US possesses cybersecurity infrastructure and capabilities that are significantly more advanced than all others but cannot alone gather the volume of intelligence it requires to carry out intelligence gathering programs pertinent to its national security. This is why the US requires information sharing programs with the Five Eyes alliance states.[352]

One of the cornerstones of cyber cooperation between both states is the Joint Defence Facility Pine Gap located outside of Alice Springs. It is used as a global satellite surveillance facility for intelligence gathering and information sharing between Five Eyes affiliated states. The facility can be understood as an indispensable resource in monitoring the threat of terrorism, nuclear proliferation and state-based cyberattacks globally.[353] Its location within Australia also serves to strengthen cyber cooperation between both states as well the alliance more broadly, particularly with the Trump administration coming into office. As Australia seeks to

[350] T. Feakin, 'The US-Australia Cyber Dialogue: prioritising cyber between strategic partners', *Australian Strategic Policy Institute*, 25 October 2016, https://www.aspistrategist.org.au/prioritising-cyber-strategic-partners-us-australia-cyber-dialogue/, accessed 18 January 2017.

[351] S. Cushing, A. Moens, A.W. Dowd, 'Cybersecurity Challenges for Canada and the United States', *Fraser Institute,* March 2015, pp. 20-23.

[352] *Ibid.*

[353] P. Dorling, 'Pine Gap's new spy role revealed', *Sydney Morning Herald,* 31 May 2015, http://www.smh.com.au/technology/technology-news/pine-gaps-new-spy-role-revealed-20150531-ghdefc.html, accessed 27 January 2017.

strengthen ties with the Trump Administration it can highlight the essential strategic value of this facility is to US interests.[354]

CHALLENGES FOR AUSTRALIA-US CYBER COOPERATION: THE CHINA WEDGE

Despite the potential for strong cyber cooperation there is the chance of challenges for deeper cyber engagement for the alliance. The major challenge Australia faces occurs as it is wedged between growing cyber disputes between China and the US. Australia has historically been able to balance a strong strategic alliance with the US whilst enjoying the economic benefits that come with China as its foremost strongest trading partner. Lum and Vaughan believe that Australia has largely felt it can balance both relationships and does not have to choose between them.[355] Cevallos, Harold and Libicki describe US-China relations as at times tense and adversarial and characterized by strategic mistrust due to a growing international rivalry for global hegemony. [356] Their diplomatic tension is currently being played out over territorial disputes in the South China Sea, friction over trade relations, human rights and the Obama Administration's foreign policy of pivoting its interests to the Asia-Pacific.[357]

Tension has been played out over cybersecurity as well. The US has long viewed China as an irresponsible and secretive actor in terms of its commitment to international norms on cybersecurity. Their relationship on cybersecurity has been characterized by a sense of deep mistrust of each other's actions in the cyber realm.[358] In recent years both states have been prone to a high degree of tension over allegations of cyberattacks and cyberespionage

[354] P. Hartcher, 'Australia has a secret weapon to keep Donald Trump in our alliance', *Sydney Morning Herald,* 15 November 2016, http://www.smh.com.au/comment/australia-has-a-secret-weapon-to-keep-donald-trump-in-our-alliance-20161114-gsor2j.html, accessed 27 January 2017.

[355] T. Lum, B. Vaughn, 'Australia: Background and U.S. Relations', *Congressional Research Service,* 14 December 2015, https://fas.org/sgp/crs/row/RL33010.pdf, accessed 20 January 2017, p. I.

[356] A.S. Cevallos, S.W. Harold, M.C. Libicki, 'Getting to yes with China in Cyberspace', *Rand Corporation,* 2016, pp. 1-2.

[357] K. Lieberthal, P.W. Singer, 'Cybersecurity and U.S.-China Relations', *Brookings Institution,* February 2012, p. 2.

[358] *Ibid,* pp. 2-6.

government and private sector interests.[359] The US has repeatedly made allegations of Chinese cyberespionage and cyberattacks on American government, military and private targets. It is the US intelligence belief that China has been conducting government-backed commercial cyberespionage on US private sector targets, stealing intellectual property to benefit its civil sector firms and to gain propriety business information.[360]

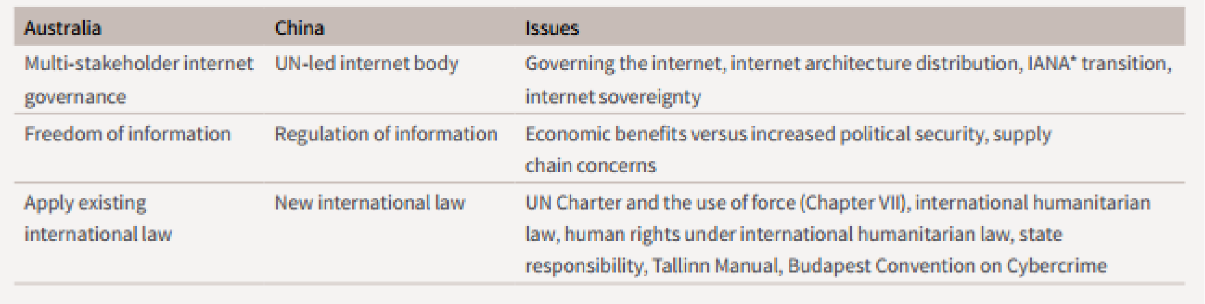
Other concerns include the allegation of traditional cyberespionage of US national security interests as well as a growing concern regarding China's cyber capabilities to launch a cyberattack on US soil that could result in potentially catastrophic damage to US critical infrastructure.[361] In the event of such an attack, the US has established preparedness to use a conventionally military response. The Cyber Incident Response Plan states that a cyberattack on a member of the defence industrial base supports US military operations: DoD is the designated to respond.[362] China has denied US allegations of hacking and cyberespionage and has in turn claimed it is a victim of US cyberattacks.[363] In recent years, China and the US have attempted to ease tension with one another through bilateral diplomatic engagement such as the 2015 US-China Cybersecurity Agreement which is viewed as the right step in establishing the framework for improved cyber relations.[364] Australian-China cyber relations itself may prove challenging in the future due to the rising concern of Chinese intelligence

[359] A.S. Cevallos, S.W. Harold, M.C. Libicki, 'Getting to yes with China in Cyberspace', *Rand Corporation,* 2016, pp. 6-8.
[360] G. Austin, 'No easy solutions in US-China cyber security', *East Asia Forum,* 6 October, 6 October 2015, http://www.eastasiaforum.org/2015/10/06/no-easy-solutions-in-us-china-cyber-security/, accessed 27 January 2017.
[361] A.S. Cevallos, S.W. Harold, M.C. Libicki, 'Getting to yes with China in Cyberspace', *Rand Corporation,* 2016,p. viii.
[362] P. Pernik, J. Wojtkowiak, A. Verschoor-Kirss, 'NATO Cyber Security Organisation: United States', NATO Cooperative Defence Centre of Excellence, pp. 21-22.
[363] K. Lieberthal, P.W. Singer, 'Cybersecurity and U.S.-China Relations', *Brookings Institution,* February 2012, pp. 4-5.
[364] S.W. Harold, 'The U.S.-China Cyber Agreement: A Good First Step', *Rand Corporation,* 1 August 2016, http://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html, accessed 28 January 2017.

services conducting cyberespionage on Australian targets such as the alleged cyberattack on the BOM in 2015.[365]

Current engagement between Australia and China on cyber policy is thin and there exists disagreement on ideological issues on how both states view international cyber norms as referred to in Figure 4.1.[366] Furthermore, Australia and China are prone to a strategic trust deficit in cyber relations which may cause challenges. One dominant view in China is that Australia and its allies are exploiting their dominance in cyberspace to undermine others.[367]

Figure 4.1: Key Australia-China ideological differences on cybersecurity



Australia	China	Issues
Multi-stakeholder internet governance	UN-led internet body	Governing the internet, internet architecture distribution, IANA* transition, internet sovereignty
Freedom of information	Regulation of information	Economic benefits versus increased political security, supply chain concerns
Apply existing international law	New international law	UN Charter and the use of force (Chapter VII), international humanitarian law, human rights under international humanitarian law, state responsibility, Tallinn Manual, Budapest Convention on Cybercrime

Source: S. Hansen, 'Special Report: Australia-China cyber relations in the next internet era', *Australian Strategic Policy Institute*, December 2015, p. 15.

CONSISTENT MESSAGING AND THE TRUMP ADMINISTRATION

A secondary long-term challenge for Australia-US cyber cooperation will be maintaining consistent messaging with one another on cybersecurity policy, especially as Australia-US relations adjust to the Trump Administration taking office. Both states would see an improvement in individual cyber maturity by promoting a consistent and persuasive narrative on cyber cooperation in a post-Snowden world. Consistent messaging between both states is

[365] C. Uhlmann, 'China blamed for 'massive' cyber attack on Bureau of Meteorology computer', *ABC News*, 2 December 2016, http://www.abc.net.au/news/2015-12-02/china-blamed-for-cyber-attack-on-bureau-of-meteorology/6993278, accessed 7 November 2016.

[366] S. Hansen, 'Special Report: Australia-China cyber relations in the next internet era', *Australian Strategic Policy Institute*, December 2015, pp. 15-16.

[367] *Ibid*, p. 7.

needed to make the case publicly for the necessity of intelligence collection as well as the secrecy which accompanies such intelligence operations.[368]

In the wake of the Snowden leaks, both states to need to be transparent about the role of intelligence in defence and security policy whilst reassuring the public that current intelligence efforts are lawful and necessary.[369] The Australian government should publicly reinstate the case for joint intelligence facilities by outlining the security benefits which come from cyber cooperation. Consistent transparent messaging is needed to rebuild the trust of regional partners following the diplomatic fallout which occurred due to the Snowden leaks.[370] A commitment to consistent messaging on cyber policy will also be beneficial as it will prevent destabilising action and miscalculation. An effort to pursue cyber norms collaboratively such as global cyber transparency will help to reinforce consistent messaging with one each other and benefit their national security interests.[371]

CONCLUSION

From the analysis in this chapter, it can be ascertained that cyber cooperation is beneficial in attaining strong cyber maturity as well as strengthening the alliance. As both states' strategic priorities have moved towards the cyber realm, cooperation has been a recent development and continues to diversify. Areas of cyber cooperation which result in strong cyber maturity are exemplified and prioritized through institutions of bilateral and multilateral engagement such as the ANZUS treaty, the Australia-US Cyber Dialogue and the Five Eyes alliance. These institutions encourage greater cyber cooperation, defence, intelligence, diplomatic and private sector cooperation as well as a clear strategic outlook on cyber policy.

[368] D. Nichola, 'Expanding Alliance: ANZUS Cooperation and Asia-Pacific security', *Australian Strategic Policy Institute*, December 2014, p. 21.

[369] *Ibid.*

[370] *Ibid.*

[371] *Ibid*, p. 22.

In cyber cooperation, Australia and the US stand to strengthen the alliance and their national security interests by advocating for international cyber norms such as a free and open internet whilst standing firm against malicious cyber threats. Key challenges in the future will be potential cyber disagreement between China and the US negatively affecting the alliance as well as maintaining consistent messaging on cyber cooperation, particularly as the Trump Administration takes office.

CONCLUSION

Following an examination of Australian and US cyber infrastructure and capabilities and their commitment to cyber cooperation, this thesis concludes that the cyber maturity of Australia is reasonably well-developed whilst US cyber maturity is extremely strong. However, there is room for improvement and challenges lie ahead. By analyzing both states' cyber governance through the scope of Chapter One's theoretical framework, this thesis finds both states are well positioned for strong cyber maturity as they have undertaken policy measures which encompass components necessary for strong cyber governance.

This thesis has argued that Australia and the US have prioritized the risk of state-based cyberattacks as higher than non-state actors in their threat evaluation. Due to their greater technological capabilities, cyberattacks by state actors pose a greater threat to national critical infrastructure than non-state actors. Additionally, state actors are prioritized as a higher threat in comparison to non-state actors due to the growing concern of cyber espionage between states. Non-state actor terrorist organizations are perceived as currently lacking the technological capabilities to commit cyberattacks with damage to cyber infrastructure. The current primary cyber threat associated with terrorist organizations is the use of the internet as a tool for recruitment, propaganda, fundraising, information sharing, mobilization and coordination. Both states have focused on undertaking a whole-of-government approach to cybersecurity in which numerous departments and agencies cooperate with one another as well as committing to international cooperation. They have addressed their domestic cyber policy agendas through national strategies which focus on CIP, cyber education and raising public awareness as well as a commitment to private sector engagement.

Australia has moderately well-developed cyber maturity but in comparison to the US has clear vulnerabilities. One critique of Australia's cyber policy, as explained by Austin and

Slay, is that Australia has failed to dedicate significant budgetary resources to national cybersecurity in comparison to other allies, such as the US. Furthermore, a criticism of Australia's cyber governance is that it has publically underscored the current threat level associated with cyberattacks in comparison to other regional allies. In the US, a challenge to cyber policy has been the inability to pass significant cyber policy legislation due to political gridlock in Washington. Both states' burden of cyber defence is mostly a healthy culture of balanced cybersecurity responsibility and authority with agencies with higher policing capabilities. This area of focus has proven to be the most significant challenge for the US due to a growing culture of competition and tension between agencies invested in cybersecurity such as the NSA, DOD, DHS, FBI and CIA. Their tension over cybersecurity jurisdiction can be understood as the result of a national cybersecurity organizational structure, which is widespread and overly bureaucratic. There is not one single authority on cybersecurity beyond the White House. This has led to tension between these agencies over whose responsibility it is to respond to cyber threats. Both Australia and the US have attempted to develop and bolster their cyber military capabilities, which indicate there is a rapid growth in cyber militarization in contemporary cyber governance.

Despite the relative infancy of cyber cooperation, this thesis has found that Australia and the US have taken great strides in committing to cyber cooperation with one another. This has been achieved through institutions such as ANZUS, the Australia-US Cyber Dialogue and Five Eyes. Both states have committed to strengthening their strategic interests through expanded information sharing, coordinated technological investment, and pledging to fight cybercrime in the Asia-Pacific. Furthermore, both states are committed to collaborating with private sector partnerships in the future. This thesis concludes that their efforts to cooperate on cybersecurity are well positioned to result in strong maturity as it exemplifies tenets of Chapter One's framework such as international cooperation, private sector engagement and norms promotion such as opposing internet censorship and defending against malicious cyber threats. This is because engagement through institutions has created strong bilateral cooperation between both states. This engagement has led to the creation of opportunities for shared private sector engagement in the Asia-Pacific as well as a commitment to fighting cybercrime bilaterally in this region. As a result of this commitment to cyber cooperation, a dialogue has evolved in which they have jointly championed the promotion of cyber norms such as internet democratization and cyber deterrence. Future challenges for Australia-US cooperation includes balancing Australia's relationship with both the China and the US and avoiding the risk of growing cyber tension compromising that balance. Furthermore, another future challenge will include maintaining consistent messaging on cyber cooperation between the Australian government and the recently inaugurated Trump Administration.

Chapter One provided a theoretical framework which the thesis uses to measure the cyber maturity of a state's cyber governance. This framework is constructed from of a literature review from contemporary cybersecurity experts in regards to what is necessary for strong state cyber maturity.

Chapter Two then uses the framework to examining the current state of Australian cyber governance. It can be concluded that in its relative infancy, the Australian government has taken significant steps to ensure strong cyber maturity. Areas it needs to continue to improve in the future is threat assessment, its commitment cyber education programs and allocating more budget resources to cybersecurity infrastructure.

Chapter Three follows the same structure and analyses the cyber governance of the US in the context of Chapter One's framework. The US is one of the global superpowers in cybersecurity and its cyber maturity can be viewed as extremely strong. Despite their overt cyber strength, criticisms of US cyber policy includes political gridlock in Washington delaying cyber legislation, debates with the private sector over the issue of encryption and tension between various intelligence and law enforcement agencies over cyber defense responsibility.

Chapter Four analyzes the recent efforts by Australia and the US to collaborate on cybersecurity through Chapter One's framework. Through collaboration via institutions such as ANZUS, The US-Australia Cyber Dialogue and Five Eyes both states stand to improve their individual cyber maturity since their cooperation exemplifies tenets of the framework such as an international cooperation, CIP, private sector engagement and a commitment to fighting cybercrime.

Despite the commendable efforts made by both states to improve and strengthen their cyber governance, new challenges and threats lie ahead in the future. The most pressing new cyber threats, which international governments will face looking ahead, includes: first, the use of soft power cyberattacks by state actors to undermine democratic institutions and influence the results of political elections to achieve their own goals of self-interest. This is often attempted through cyber espionage and dissemination of sensitive information.[372] Second, disagreement exists between national governments, the private sector and the public over government and law enforcement agencies ability to access cryptographically protected technology for reasons pertinent to national security, counterintelligence and law enforcement.[373] Furthermore, this debate will continue as the public and state actors campaign for their right to access to cryptography strong enough to resist decryption by national intelligence agencies.[374] Third, the growing threat of non-state terrorist organizations technological

[372] M. Aaolta, M. Mattiisen, Election Hacking in Democracies: The Example of The U.S. 2016 Elections, *The Finnish Institute of International Affairs*, FIIA Briefing Paper 204, October 2016, pp. 6-8.

[373] C. Cordero, M. Zwillinger, 'Should Law Enforcement Have the Ability to Access Encrypted Communications?', *Wall Street Journal*, 19 April 2015, https://www.wsj.com/articles/should-law-enforcement-have-the-ability-to-access-encrypted-communications-1429499474, accessed 25/3/2017.

[374] J.V. Hoboken, W. Shulz, 'Human Rights and Encryption', UNESCO Series on Internet Freedom, *UNESCO Publishing*, 2016, pp. 9-11.

capabilities are likely to improve to the level that they gain the ability to launch cyberattacks, which could cause disastrous damage to critical infrastructure.[375] Fourth, the risk of further escalating tension between state actors over the proliferation of cyberattacks and cyberespionage could result in the conventional military responses and conflict as a retort to malicious cyber threats.[376] Fifth, the risk exists of the Trump Administration failing to sustain cyber governance. Complacent and inept cyber governance could leave the US and its allies vulnerable to malicious cyberattacks with disastrous consequences for critical infrastructure.[377] While significant challenges lie ahead, Australia and US cyber maturity strength will provide the basis from which these challenges can be addressed.

[375] P.W. Singer, 'The Cyber Terror Boogeyman', *Brookings Institution*, 1 November 2012, https://www.brookings.edu/articles/the-cyber-terror-bogeyman/, accessed 10 September 2016.

[376] S. Alarcon, ‘War over Cyber Attacks is Possible but Unlikely’, *Stanford Political Journal*, 2 March 2016, https://stanfordpolitics.com/war-over-cyber-attacks-is-possible-but-unlikely-95a854a4e3c5#.jx6rg5d29, accessed 25 March 2017.

[377] Y. Tadjdeh, ‘Trump to Face Major Cybersecurity Challenges’, *National Defense Magazine*, February 2017, http://www.nationaldefensemagazine.org/archive/2017/february/Pages/TrumptoFaceMajorCybersecurityChallenges.aspx, accessed 25 March 2017.

BIBLIOGRAPHY

Primary Sources

(a) Government Reports and Publications

'2016 Cyber Security Strategy', *Commonwealth of Australia 2016*.

Australian Cyber Security Centre, 2016 Threat Report, Australian Federal Government, 2016.

Australian Cyber Security Centre, 'Frequently-Asked Questions', *Commonwealth of Australia 2016,* https://www.acsc.gov.au/faqs.html, accessed 4 November 2016.

Australian Signals Directorate, 'ACSC- Australian Cyber Security Centre', *Commonwealth of Australia 2017,* https://www.asd.gov.au/about/roleinfosec.htm, accessed 8 April 2017.

Australian Signals Directorate, 'Information Security (Infosec) Role', *Commonwealth of Australia 2017,* https://www.asd.gov.au/about/roleinfosec.htm, accessed 8 April 2017.

Australian Signals Directorate, 'UKUSA Allies', *Commonwealth of Australia 2016*, 2016, http://www.asd.gov.au/partners/allies.htm, accessed 5 November 2016.

Bund, J., 'Cybersecurity and Democracy: Hacking, Leaking and Voting', European Union Institute for Security Studies, Brief Issue, No. 30, November 2016, pp. 1-4.

Cavelty, M.D., 'The Militarisation of Cyberspace: Why Less May Be Better', 4th International Conference on Cyber Conflict', *NATO CCD COE Publications*, 2012, p. 141.

Cilluffo, F.J., 'Testimony on Emerging Cyber Threats to the United States before the US House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Securities Technology', 2016, http://docs.house.gov/meetings/HM/HM08/20160225/104505/HHRG-114-HM08-Wstate-

CilluffoF-20160225.pdf, accessed 10 December 2016, pp. 1-4.

‘Cyber-security strategy funding fact sheet’, *Commonwealth of Australia 2016.*

Department of Homeland Security, ‘DHS Launches National Initiative for Cybersecurity Careers and Studies’, 21 February 2013, https://www.dhs.gov/news/2013/02/21/dhs-launches-national-initiative-cybersecurity-careers-and-studies, accessed 27 December 2016.

Department of Homeland Security, ‘Cybersecurity’, 27 September 2016, https://www.dhs.gov/topic/cybersecurity, accessed 20 December 2016.

Department of Homeland Security, ‘Office of Cybersecurity and Communications’, 6 October 2016, https://www.dhs.gov/office-cybersecurity-and-communications, accessed 20 December 2016.

Federal Bureau of Investigation, ‘What we investigate: Cyber Crime’, 2016, https://www.fbi.gov/investigate/cyber, accessed 20 December 2016.

Fischer, E.A., ‘Cybersecurity Issues and Challenges: In Brief’, *Congressional Research Service*, 12 August 2016.

Hoboken, J.V., and Shulz, W., ‘Human Rights and Encryption’, UNESCO Series on Internet Freedom, *UNESCO Publishing,* 2016, pp. 9-11.

Holl Lute, J., ‘Testimony on DHS Cybersecurity: Roles and Responsibilities to Protect the Nation’s Critical Infrastructure to the US House of Representatives Committee on Homeland Security, 13 March 2013, file://usergh/h/hold0085/Downloads/nps59-032913-02%20(2).pdf, pp. 1-10.

Information Security Policy Council (Japan), ‘International Strategy on Cybersecurity Cooperation: J-initiative for Cybersecurity’, *National Center of Incident Readiness and Strategy for Cybersecurity*, 2 October 2013, pp. 1-2.

Lum T., and Vaughn, B., ‘Australia: Background and U.S. Relations’, *Congressional Research Service*, 14 December 2015, https://fas.org/sgp/crs/row/RL33010.pdf, accessed 20 January 2017.

National Counter-Terrorism Committee, ‘National Counter-Terrorism Plan’, *Commonwealth of Australia 2012*.

National Security Agency, ‘What we do: Cyber’, 3 May 2016, https://www.nsa.gov/what-we-do/cyber/, accessed 20 December 2016.

Office of the Director of National Intelligence, ‘Assessing Russian Activities and Intentions in Recent US Elections’, *Intelligence Community Assessment*, 6 January 2017, pp. i-iii.

Office of the Director of National Intelligence, ‘Cyber Threat Intelligence Integration Center: Who we are’, 2015, https://www.dni.gov/index.php/about/organization/ctiic-who-we-are, accessed 20 December 2016.

Office of the Press Secretary, ‘Fact Sheet: Cybersecurity National Action Plan’, 9 February 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan, accessed 24 December 2016.

Office of the Press Secretary, ‘Fact Sheet: US – EU Cyber Cooperation’, 26 March 2014, https://www.whitehouse.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation, accessed 21 December 2016.

Office of the Press Secretary, ‘Joint Fact Sheet: The United States – Republic of Korea Alliance: Shared Values, New Frontiers’, 16 October 2015, https://www.whitehouse.gov/the-press-office/2015/10/16/joint-fact-sheet-united-states-republic-korea-alliance-shared-values-new, accessed 21 December 2016.

Office of the Press Secretary, ‘Joint Statement: 2015 United States-India Cyber Dialogue’, 29 September 2016, https://www.whitehouse.gov/the-press-office/2016/09/29/joint-statement-2016-united-states-india-cyber-dialogue, accessed 21 December 2016.

Office of the Press Secretary, ‘Fact Sheet: United States – Australia Cooperation: Deepening our Strategic Partnership’, 19 January 2016, https://www.whitehouse.gov/the-press-office/2016/01/19/fact-sheet-united-states-%E2%80%93-australia-cooperation-deepening-our-strategic, accessed 21 December 2016.

Office of the Press Secretary, ‘Fact Sheet: US – United Kingdom Cybersecurity Cooperation, 16 January 2015, https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation, accessed 21 December 2016.

Perl, R., ‘The Department of Homeland Security: Background and Challenges’, Terrorism: Reducing Vulnerabilities and Improving Responses: US – Russia Workshop Proceedings, National Academies Press, 2004, pp. 176-178.

Pernik, P., Wojtkowiak, J., and Verschoor-Kirss, A., ‘NATO Cyber Security Organisation: United States’, *NATO Cooperative Defence Centre of Excellence*, p. 15

Public Safety Canada, ‘Cybersecurity Action Plan between Public Safety Canada and the Department of Homeland Security’, 2 December 2015, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-en.aspx, accessed 21 December 2016.

Rollins, J.W., and Theohary, C.A., 'Cyberwarfare and Cyberterrorism: In Brief', *Congressional Research Service*, 17 March 2015, https://fas.org/sgp/crs/natsec/R43955.pdf, accessed 1 September 2016, pp. 1-4.

Rudd, K., 'Cooperation on Cyber – a new dimension of the US alliance', *Former Minister for Foreign Affairs: The Hon Kevin Rudd MP*, 15 September 2011, http://foreignminister.gov.au/releases/Pages/2011/kr_mr_110916.aspx?ministerid=2, accessed 21 January 2017.

United Nations Office on Drugs and Crime, 'The Use of the Internet for Terrorist Purposes', *United Nations*, 2012, pp. 3-6.

United States Computer Readiness Team, 'About Us', 2016, https://www.us-cert.gov/about-us, accessed 20 December 2016.

US Department of Homeland Security, 'National Infrastructure Protection Plan', 2016, https://www.dhs.gov/national-infrastructure-protection-plan, accessed 11 December 2016.

US Department of Justice, 'Cybersecurity Unit', 21 November 2016, https://www.justice.gov/criminal-ccips/cybersecurity-unit, accessed 20 December 2016.

US Department of State, 'Department of State International Cyberspace Policy Strategy', March 2016, pp. 1-12.

US Department of State, 'The 4th US-Japan Bilateral Cyber Dialogue', 27 July 2016, https://www.state.gov/r/pa/prs/ps/2016/07/260572.htm, accessed 21 December 2016.

US Department of Defense, 'All Cyber Mission Force Teams Achieve Initial Operating Capability', *US Department of Defense*, 24 October 2016, https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability, accessed 9 April 2017.

US Department of Defense, ‘Fiscal Year 2017 Budget Fact Sheet’, 2016, https://www.defense.gov/Portals/1/features/2016/0216_budget/docs/2-4-16_Consolidated_DoD_FY17_Budget_Fact_Sheet.pdf, accessed 28 December 2016. p 5.

US Department of Defense, ‘The Department of Defense Cyber Strategy’, 2015.

US Department of Defense, ‘The DoD Cyber Strategy’, April 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, accessed 28 December 2016, p. 5.

Wadell, A.P., ‘Cooperation and Integration among Australia’s National Security Community’, *Studies in Intelligence*, Vol. 59, No. 3, September 2015, pp. 26-32.

(b) Non-Government Reports and Publications

Australian Strategic Policy Institute, 'Cyber Maturity in the Asia-Pacific Region 2015', *Australian Strategic Policy Institute*, 2015.

Australian Strategic Policy Institute, ‘Cyber Maturity in the Asia-Pacific Region 2016, *Australian Strategic Policy Institute*, 2016.

ASPI International Cyber Policy Centre, ‘ASPI and CSIS to bring together new Australia-US Cyber Dialogue’, *Australian Strategic Policy Institute,* 20 January 2016, https://www.aspistrategist.org.au/aspi-and-csis-to-bring-together-new-australia-us-cyber-security-dialogue/, accessed 22 January 2017.

Austin, G., and Slay, J., 'Australia's Response to Advanced Technology Threats: An Agenda for the next Government', *Australian Center For Cyber Security*, May 2016.

Cushing, S., Moens, A., and Dowd, A.W., ‘Cybersecurity Challenges for Canada and the United States’, *Fraser Institute*, March 2015, pp. 20-23.

Davies, A., ‘An Australian Perspective on ANZUS and cyberthreats’, ANZUS 2.0: Cybersecurity and Australia-US Relations, *Australian Strategic Policy Institute*, 2012.

Davies, A., Herrera-Flanigan, J., Khalil, L., Lewis, J., and Mulvenon, J., ‘ANZUS 2.0: Cybersecurity and Australia-US relations’, *Australian Strategic Policy Institute*, April 2016, Issue 46, pp. 1-3.

Davies, A., and Jennings, P., ‘Expanding Alliance: ANZUS Cooperation and Asia-Pacific security’, *Australian Strategic Policy Institute*, 2014, pp. 5-7.

Feakin, T., and Jennings, P., 'The Emerging Agenda for Cybersecurity', *Australian Strategic Policy Institute*, July 2013.

Feakin, T., ‘The US-Australia Cyber Dialogue: prioritising cyber between strategic partners’, *Australian Strategic Policy Institute*, 25 October 2016, https://www.aspistrategist.org.au/prioritising-cyber-strategic-partners-us-australia-cyber-dialogue/, accessed 18 January 2017.

Fontaine, R., ‘Against Complacency: Risks and Opportunities for the Australia-US Alliance’, *United States Studies Centre*, October 2016, p. 4.

Ford, R., and Gordon, S., ‘Cyberterrorism?’, Symantec Security Response White Paper, *Symantec*, August 2003, pp. 3-4.

Gribbon, L., Horvath, V., Robertson, K., and Robinson, N., 'Cyber-security Threat Characterisation: A Rapid Comparative Analysis', RAND Corporation, 2013.

Hansen, S., ‘Special Report: Australia-China cyber relations in the next internet era’, *Australian Strategic Policy Institute*, December 2015, pp. 15-16.

Hawkins, Z., ‘The US-Australia Cyber Dialogue: cooperation in the Asia-Pacific’, *Australian Strategic Policy Institute*, 1 November 2016, https://www.aspistrategist.org.au/us-australia-cyber-dialogue-cooperation-asia-pacific/, accessed 21 January 2017.

Hawkins, Z., and Nevill, L., ‘The US-Australia Cyber Dialogue: fighting cybercrime in the Asia-Pacific’, *Australian Strategic Policy Institute*, 4 November 2016, https://www.aspistrategist.org.au/us-australia-cyber-dialogue-fighting-cybercrime-asia-pacific/, accessed 23 January 2017.

Lieberthal, K., Singer, P.W., ‘Cybersecurity and U.S.-China Relations’, *Brookings Institution*, February 2012, pp. 2-6.

MacGibbon, A., 'Cyber Security: Threats and Responses in the Information Age', *Australian Strategic Policy Institute*, December 2009, Issue 26.

Medcalf, R., Sussex, M., Tsirbas, M., Young, and R., ‘The Trump Presidency and Australia’s security: don’t panic, don’t relax’, *National Security College (ANU)*, Policy Options Paper, No. 1, January 2017, p. 2.

Nichola, D., ‘Expanding Alliance: ANZUS Cooperation and Asia-Pacific security’, *Australian Strategic Policy Institute*, 2014.

Rogers, Z., ‘ASCS 2017 Report: Australian Cyber Security Centre Conference”, *Flinders University Centre for United States and Asia Policy Studies*, 20 March 2017.

Weimann,G., 'Cyberterrorism: How Real is The Threat?', *United States Institute of Peace*, December 2004, https://www.usip.org/sites/default/files/sr119.pdf, accessed 4 September 2016, pp. 2-3.

(c) Newspaper and Media Sources

Ackerman, S., and Thielman, S., ‘US officially accuses Russia of hacking DNC and interfering with election’, *The Guardian*, 9 October 2016.

Austin, G., ‘Australia still doesn’t see a cyber attack as the menace our allies fear’, *The Conversation*, April 25 2016, https://theconversation.com/australia-still-doesnt-see-a-cyber-attack-as-the-menace-our-allies-fear-57719, accessed 10 November 2016.

Bennett, B.W., ‘Did North Korea Hack Sony?’, *Rand Corporation*, 11 December 2014, http://www.rand.org/blog/2014/12/did-north-korea-hack-sony-pictures-entertainment.html, 16 December 2016.

Berman, R., ‘The Hacking of Central Command’, *The Atlantic*, 12 January 2015, https://www.theatlantic.com/politics/archive/2015/01/central-command-accounts-are-hacked-centcom-isis-soldiers-obama-cybersecurity-cybercaliphate/384442/, accessed 18 December 2016.

Besser, L., Stumer, J., and Sveen, B., ‘Government computer networks breached in cyber attack as experts warn of espionage threat’, *ABC News*, 29 August 2016, http://www.abc.net.au/news/2016-08-29/chinese-hackers-behind-defence-austrade-security-breaches/7790166, accessed 7 November 2016.

Brown, J., ‘Australia-US Defence Deal: What it means’, *The Lowy Institute*, 13 June 2014, https://www.lowyinstitute.org/the-interpreter/australia-us-defence-deal-what-it-means, accessed 20 January 2017.

Bucci, N., ‘Islamic State posts Australian hit list after hacking addresses, mobile numbers’, 12 August 2015, http://www.smh.com.au/national/islamic-state-posts-australian-hit-list-after-hacking-addresses-mobile-numbers-20150812-gixrmz.html, accessed 7 November 2016.

Bumiller,E., and Shanker, T., ‘Panetta Warns of Dire Threat of Cyberattack on US’, *New York Times*, 11 October 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=1, accessed 5 September 2016.

Cordero, C., and Zwillinger, M., ‘Should Law Enforcement Have the Ability to Access Encrypted Communications?’, *Wall Street Journal,* 19 April 2015, https://www.wsj.com/articles/should-law-enforcement-have-the-ability-to-access-encrypted-communications-1429499474, accessed 25/3/2017.

Davies, A., ‘Cyber Wrap Special: two heads are better than one’, *Australian Strategic Policy Institute,* 21 September 2016, https://www.aspistrategist.org.au/cyber-wrap-special-two-heads-better-one/, accessed 28 December 2016.

Dodds, P., and Perry, N., ‘Five Eyes spying alliance will survive Edward Snowden: experts’, *Sydney Morning Herald,* 18 July 2013, http://www.smh.com.au/it-pro/security-it/five-eyes-spying-alliance, accessed 5 April 2017.

Dupont, A., 'Cybersphere is the Globe's New Battlefront', *The Lowy Institute*, 26 April 2016, http://www.lowyinstitute.org/publications/cybersphere-globes-new-battlefront, accessed 24 September 2016.

Emspak, J., ‘Feuding agencies agree to disagree on cybersecurity’, *NBC News*, 31 August 2011, http://www.nbcnews.com/id/44350731/ns/technology_and_science-security/t/feuding-agencies-agree-disagree-cybersecurity/#.WKjnwW-GPIU, accessed 23 September 2016.

Entous, A., and Nakashima, E., ‘Divisions between CIA, FBI surface in debate over Russian motives in election hack’, *Chicago Tribune,* 10 December 2016, http://www.chicagotribune.com/news/nationworld/politics/ct-russian-election-tampering-cia-fbi-20161210-story.html, accessed 19 February 2017.

Gady, F.S., ‘Top US Spy Chief: China still Successful in Cyber Espionage against US’, 16 February 2016, in *The Diplomat*, 2016, http://thediplomat.com/2016/02/top-us-spy-chief-china-still-successful-in-cyber-espionage-against-us/, accessed 9 December 2016.

Harold, S.W., ‘The U.S.-China Cyber Agreement: A Good First Step’, *Rand Corporation,* 1 August 2016, http://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html, accessed 28 January 2017.

Hasan, M., ‘International Cyber Security Cooperation’, *Modern Diplomacy,* 13 November 2016, http://moderndiplomacy.eu/index.php?option=com_k2&view=item&id=1894:international-cyber-security-cooperation&Itemid=154, accessed 18 January 2017.

Hawkins, Z., Nevill, L., ‘National cyber budgets’, same, same but different’, *Australian Strategic Policy Institute,* 16 June 2016, https://www.aspistrategist.org.au/national-cyber-budgets-different/, accessed 20 September 2016.

Herszenhorn, D.M., ‘Europe braces for Russia hacking in upcoming elections’ *Politico,* 13 December 2016, http://www.politico.eu/article/europe-russia-hacking-elections/, accessed 19 February 2017.

Lewis, J.A., 'Sony and North Korea: Making the Case', *Center for Strategic and International Studies*, 5 December 2014, https://www.csis.org/analysis/sony-and-north-korea-making-case, accessed 16 December 2016.

Marks, J., 'ISIL aims to launch cyberattacks on US', *Politico,* 29 December 2015, http://www.politico.com/story/2015/12/isil-terrorism-cyber-attacks-217179, accessed 18 December 2016.

Miller, G., 'CIA plans major reorganization and a focus on digital espionage', *Washington Post,* 6 March 2015, https://www.washingtonpost.com/world/national-security/cia-plans-major-reorganization-and-a-focus-on-digital-espionage/2015/03/06/87e94a1e-c2aa-11e4-9ec2-b418f57a4a99_story.html?utm_term=.d82ff692a6c0, accessed 20 December 2016.

Nakashima, E., 'Obama to be urged to split cyberwar command from NSA', *Washington Post,* 13 September 2016, https://www.washingtonpost.com/world/national-security/obama-to-be-urged-to-split-cyberwar-command-from-the-nsa/2016/09/12/0ad09a22-788f-11e6-ac8e-cf8e0dd91dc7_story.html?utm_term=.e6dbb84132a3, accessed 23 December 2016.

Nevill, L., 'Cyber security in the 2015 Defence White: a preview", *Australian Strategic Policy Institute*, 2 July 2015, https://www.aspistrategist.org.au/cyber-security-in-the-2015-defence-white-paper-a-preview/, accessed 8 April 2017.

Nicholson, B., 'Five Eyes saving lives', *The Australian,* 20 November 2013, http://www.theaustralian.com.au/news/inquirer/five-eyes-saving-lives/news-story/c365f88578b16a97b6e874c6c503b4ae, accessed 5 April 2017.

Paletta, D., Valentino-Devries, J., and Yadron, D., 'Cyberwar ignites a new arms race', in *The Wall Street Journal*, 11 October 2015, http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128, accessed 5 December 2016.

Perlroth, N., and Sanger, D.E., ‘US Said to Find North Korea Ordered Cyberattack on Sony’, *New York Times*, 17 December 2014, https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html, accessed 16 December 2016.

Slay, J., ‘Australia is vulnerable to cyber threats, so what can we do about it’, *The Conversation*, 12 October 2016, https://theconversation.com/australia-is-vulnerable-to-cyber-threats-so-what-can-we-do-about-it-66903, accessed 7 April 2017.

Singer, P.W., 'The Cyber Terror Boogeyman', *Brookings Institution*, 1 November 2012, https://www.brookings.edu/articles/the-cyber-terror-bogeyman/, accessed 10 September 2016.

Tadjdeh, Y., ‘Trump to Face Major Cybersecurity Challenges’, *National Defense Magazine*, February 2017, http://www.nationaldefensemagazine.org/archive/2017/february/Pages/TrumptoFaceMajorCybersecurityChallenges.aspx, accessed 25 March 2017.

Tanter, R., ‘Fifty years on, Pine Gap should reform to better serve Australia’, *The Conversation*, 9 December 2016, http://theconversation.com/fifty-years-on-pine-gap-should-reform-to-better-serve-australia-65650, accessed 10 December 2016.

Timm, T., ‘The rush to blame Russia for the DNC email hack is premature’, in *The Guardian*, 26 July 2016, https://www.theguardian.com/commentisfree/2016/jul/25/russia-blame-dnc-email-hack-premature, accessed 15 December 2016.

Uhlmann, C., ‘China blamed for ‘massive’ cyber attack on Bureau of Meteorology computer’, *ABC News*, 2 December 2016, http://www.abc.net.au/news/2015-12-02/china-blamed-for-cyber-attack-on-bureau-of-meteorology/6993278, accessed 7 November 2016.

Wadell, K., ‘Don’t panic (for now) about ISIS hacking’, in *The Atlantic*, 28 April 2016, http://www.theatlantic.com/technology/archive/2016/04/dont-panic-for-now-about-isis-hacking/480282/, accessed 18 December 2016.

Wallace, I., 'Cyber Security: Why Military Forces should take a Back Seat', *The Lowy Interpreter,* 21 October 2013, http://www.lowyinterpreter.org/post/2013/10/21/Cyber-security-Why-military-forces-should-take-a-back-seat.aspx, accessed 23 September 2016.

Wallace, I., 'The Military Role in National Cybersecurity Governance', *Brookings Institution*, 16 December 2013, https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/, accessed 23 September 2016.

Wroe, D., ‘Jihadists could launch major cyber attacks, says former ASIO boss David Irvine’, in *Sydney Morning Herald,* 26 October 2016, http://www.smh.com.au/federal-politics/political-news/jihadists-could-launch-major-cyber-attacks-says-former-asio-boss-david-irvine-20151026-gkisup.html, accessed 7 November 2016.

Yadron, D., ‘US efforts to regulate encryption have been flawed, government reports find’, *The Guardian*, 30 June 2016, www.theguardian.com/technology/2016/jun/29/government-encryption-regulation-report-criticism, accessed 24 December 2016.

(d) Other Primary Sources

Kelton, M., ‘Arresting diffusion: Evolving spatial domains of power in the Australia-US alliance’, Paper for the ISA Annual Convention, San Francisco, 3-6 April 2013, p. 10.

Secondary Sources

(a) Books

Bronk, C., ‘Cyber Threat: The Rise of Information Geopolitics in US National Security, ABC-CLIO, 2016, p. 57.

(b) Chapters in Edited Collections

Akhgar, B., Bosco, F., and Staniforth, A., Cyber Crime and Cyber Terrorism Investigator's Handbook, Syngress, 2014. pp. 40-41.

Ariely, A., ‘Adaptive Responses to Cyberterrorism’, Cyberterrorism: Understanding, Assessment, and Response, Springer Publishing, 2014.

Clark, D., Diffie, W., and Sofaer, A.D., ‘Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy’, National Academies Press, 2010, pp. 184-185.

C. Uhoff, ‘Strategic Cyber Intelligence: An Examination of Practices across Industry, Government and Military’, Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practise, Palgrave Macmillan, 2015, pp. 205-2015.

(c) Journal Articles

Alarcon, S., ‘War over Cyber Attacks is Possible but Unlikely’, *Stanford Political Journal*, 2 March 2016, https://stanfordpolitics.com/war-over-cyber-attacks-is-possible-but-unlikely-95a854a4e3c5#.jx6rg5d29, accessed 25 March 2017.

Carlin, J.P., ‘Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats’, in *Harvard National Security Journal*, Vol. 7, 2016, pp. 393-398.

Hunker, J.A., and Kelly, T.K., 'Cyber Policy: Institutional Struggle in a Transformed World', *I/S: A Journal of Law and Policy for the Information Society*, Vol. 8, No. 2, Fall 2012, pp. 214-215.

Jennings, P., ‘The 2016 Defence White Paper and the ANZUS Alliance’, *Security Challenges*, Vol. 12, No. 1, 2016, p. 53.

Leuprecht, C., Skillicorn, D.B., V.E. Tait, ‘Beyond the Castle Model of cyber-risk and cyber-security’, *Government Information Quarterly,* Elsevier, 2016, pp. 1-3.

Matusitz, J., ‘Cyberterrorism: How Can American Foreign Policy Be Strengthened In The Information Age?’, *American Foreign Policy Interests,* Vol. 27, No. 2, April 2005, p. 137.

Waters, G., ‘The Case for a Regional Cyber Security Action Task Force’, *Institute for Regional Security,* Security Challenges, Vol. 7, No. 1, Autumn 2011, p. 4.

Weimann, G., 'Cyberterrorism: The Sum of All Fears?', *Studies in Conflict & Terrorism*, Vol. 28, 2005, pp. 130-140.

(d) Other Secondary Sources

Organizations and Institutions that Address International Cybersecurity’, *Information Technology Industry Council*, 2016, http:/www.itic.org/dotAsset/c/c/cc91d83a-e8a9-40ac-8d75-0f544ba41a71.pdf, accessed 10 September 2016.

Pethia, R.D., Van Wyk, K.R., ‘Computer Emergency Response – An International Problem’, Computer Emergency Response Team, Software Engineering Institute, *Carnegie Mellon University*, 1990, pp. 2-3.

Von Knop, K., ‘Institutionalization of a Web-Focused, Multinational Counter-Terror Campaign’, Responses to Cyber Terrorism’, *Centre of Excellence Defence Against Terrorism*, 2008, p.16.