2024

Deterring the Digital Dragon

Bryn Lacey

DETERRING THE DIGITAL DRAGON: CHINA, AUSTRALIA AND CYBERSECURITY

Bryn Lacey

Submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

School of Arts and Sciences

Fremantle Campus

March 2024

Declaration of Authorship

To the best of the candidate's knowledge, this thesis contains no material previously published by another person, except where due acknowledgment has been made.

This thesis is the candidate's own work and contains no material which has been accepted for the award of any other degree or diploma in any institution.

24/10/2024

X [redacted]

Bryn Lacey

Signed by: Bryn Lacey

Bryn Lacey

10th October, 2024

Abstract

Australia's 21st century has been heavily influenced by a growing number of cyber incidents ranging from individuals causing extraordinary damage to state-based attacks from adversary states such as China. Focusing on state actors in the cyber domain, this thesis investigates Martin Libicki's cyber-deterrence framework, with a specific emphasis on the employment of deterrence by punishment, and applies this concept to the case study of the relationship between Australia and China.

In recent years, Australia has been consistently targeted by sophisticated state-based cyber actors and the Australian Government has appeared increasingly prepared to publicly criticise Beijing as a key security challenge. Meanwhile, ideas related to cyber deterrence are becoming even more complicated because the field of interstate competition is expanding. With states such as China putting more effort into seeking advantage through means that fall just short of war, countries such as Australia are continuing to seek to formulate more sophisticated, relevant concepts of deterrence that include establishing thresholds, communicating threats and attributing accurately.

Overall, a range of cyber incidents have highlighted the increasing need for Australia to have a robust deterrence framework that can affect the strategic thoughts and policy processes of China. Further, Australia and China do often appear to have contradictory outlooks on the cyber domain and how states should approach it which has led to diplomatic contestation. Nonetheless, deterrence strategies, including by punishment, aim to reduce the likelihood of conflict and attempt to establish thresholds that states can adhere to while understanding the ramifications of political actions.

Yet, various obstacles and challenges will make deterrence by punishment an ongoing policy challenge in cyberspace, but also potentially destabilising in terms of efforts to constrain state behaviour especially given the background of broader geopolitical tensions between Australia and China. The thesis will argue that the prospect of 'successful' deterrence in cyberwarfare does exist for Australia, at least in part and under particular circumstances against China and that Libicki's framework is a useful policy tool for Australia. It will also present potential simulations exercises that decision-makers in Australia could utilise.

Acknowledgements

To my supervisor, Daniel Baldino, this has been a crazy ride – for me at least. I can't imagine Daniel has had to look after a candidate with the same rollercoaster of a journey either. Daniels patience, care, effort, attention to detail and overall excellence has been instrumental in me reaching this final stage. It hardly feels real but it is heavily in thanks to him. A fitting capstone on a period of intense struggle is to have such a moment of celebration. Thank you.

Martin Drum has been an exceptional rock in the background, providing both myself directly and Daniel the necessary wisdom and – at times with me at least – just the right amount of touch to settle the nerves and steady my ship. Without Martin's contributions and grace in picking up when Daniel himself was otherwise occupied, I have been indebted to Martin since the earliest inception of my entire journey at Notre Dame – me cold calling for work as a struggling tutor and Martin introducing me to Daniel as fate would have it.

Mum and Dad you probably believe this less than me! I am constantly in awe of your patience and love, and I know it and appreciate it. Strength starts from the grip but when I lost mine, I had the best support any person could ask for to hold me and keep me on course. You are, as always, my inspiration to be a better father.

Quentin Beresford and Genevieve Hohnen are responsible for getting me into this whole academic life – and I'm sure we'll enjoy a laugh about that soon enough. I look forward to sharing this with them in person in the coming days, weeks, months or years. We've got nothing but time now on that front, and no more deadlines.

Abi, you are the light of my life, and this is more than anyone dedicated to you. Seeing you take up reading with such skill and ease reminds me of the simple joy of words and that we can engage in our language for pleasure and not just for study. I can't wait to read with you forever. I love you.

To all my friends and family, thank you.

Bryn

This research was supported by an Australian Government Research Training Programme Scholarship.

Table of Contents

Declaration of Authorship ..... **ii**
Abstract ..... **iii**
Acknowledgements ..... **iv**
Table of Contents ..... **v**
List of Figures ..... **xii**
List of Abbreviations ..... **xiii**
Chapter 1: Introduction **1**
1.1 Research Aims, Context, Methodology and Objectives 6
1.2 Background 14
1.3 Significance 16
1.4 Limitations 20
1.5 Literature Review 23
1.6 Deterrence Strategy and the Cyber World 25
1.7 Deterrence by Punishment Frameworks with Cyber Purposes 30
1.8 Conventional Deterrence 32
1.9 Extended Deterrence 34
1.10 Cyber Deterrence, Risk Management and Cybersecurity 35
1.11 Moving Forward 40
Chapter 2: Cybersecurity Policy Developments in Australia **41**
2.1 Introduction 41
2.2 Key Policy Challenges 43
2.3 White Paper in 2000 and Peripherals 47
2.4 Defence White Paper in 2009: Defending Australia in the Asia-Pacific Century 53
2.5 Australia's 2016 Cyber Security Strategy and Defence White Paper 58
2.6 Australia's Cyber Security Strategy 2020 66
2.7 Force Update in 2020 71
2.8 REDSPICE 74
2.9 Year 2022, New Government and the Deluge of Data Breaches 77
2.10 Conclusion 82
Chapter 3: China's Cyber Strategy **87**
3.1 Introduction 87
3.2 Chinese Actions as a Cyberthreat 90
3.3 Unrestricted Warfare in 1999 95
3.4 Science of Military Strategy 97
3.5 Science of Military Strategy, 2013 100
3.6 Defence White Paper 2015 104
3.7 General Staff Department, 3/PLA 108
3.7.1 Unit 61398 109
3.7.2 Unit 61486 110
3.8 General Staff Department, 4/PLA 112
3.9 PLA Cyberwarfare Evolution in Preparation for the Strategic Support Force 112
3.10 Ministry of State Security 115
3.10.1 APT 10 116

3.10.2 APT 3 117
3.11 Defence White Paper in 2019 119
3.12 Science of Military Strategy in 2017 and 2020 121
3.13 Conclusion 124

Chapter 4: Australia's Attribution 'Who did it' Capability and Strategy 127
4.1 Introduction 127
4.2 Risk Assessments and Responses 130
4.3 How Sophisticated Are Cyber Attacks? 132
4.4 Australian Context and the 'Name and Blame' Game 135
4.5 Caveats 142
4.6 Attribution Models and Deterrence in the Cyber Era 145
4.7 Legitimacy and Why Is Attribution Significant for Policymakers? 149
4.8 Australia's Capacity and Attribution Examples 152
4.8.1 Living Off the Land to Avoid Detection 153
4.8.2 LockBit 3.0 154
4.8.3 BianLian Ransomware Group 155
4.9 Ramifications for Libicki's Deterrence Framework 156
4.9.1 Do We Know Who Did It? 156
4.9.2 Will Third Parties Join the Fight? 157
4.9.3 Does Retaliation Send the Right Message to Our Own Side? 158
4.9.4 Can We Avoid Escalation? 159
4.10 Summary 161

Chapter 5: Deploy Payload—Destroy, Disrupt and Degrade Target Enemy Networks 163
5.1 Australia, China and the Logic of Retaliation 165
5.2 Deterrence by Punishment and Decision-making in the Cyber Context 166
5.3 Different Threat Actors 168
5.4 Deterrence and Punishment 174
5.5 Communication, Capacity and Deterrence by Punishment 176
5.6 A Deploy Payload Blueprint: Destroy, Disrupt and Degrade Target Chinese Networks 179
5.7 Punishment Frameworks and What Was the Original Purpose of the Attack? 185
5.8 Unpacking the Punishment Framework 187
5.8.1 Can We Hold Their Assets at Risk? 188
5.8.2 Assessment 193
5.9 Conclusion 194

Chapter 6: Conclusion and Discussion 195
6.1 The Research Question 195
6.2 Contribution to Knowledge: Conceptualising Cybersecurity and Risk Strategy 197
6.2.1 Attribution of Cyber Attacks 199
6.2.2 Risk Assessment of Offensive Effects 199
6.2.3 Approved Offensive Effects (Political Will/Credibility) 200
6.2.4 Desired Offensive Effects Sent to Technical Teams 200
6.2.5 Technically Possible Actions 200
6.2.6 Technically Possible Offensive Effects Sent to Communications 201
6.2.7 Effect That Can Be Threatened That Decision-makers Know Are Within Escalation and Technical Capability: 201
6.2.8 Ability to Communicate Effects 201
6.2.9 Unacceptable Cascade Effects 202

6.2.10 Review Discarded Effects and Test for Utility: 202
6.2.11 Strategic Review (Process End, Continuous Improvement Feedback to Brainstorm) 202
6.3 Research Findings from SWOT Analysis 202
6.3.1 Do We Know Who Did It? 203
6.3.1.1 Strengths 203
6.3.1.2 Weaknesses 203
6.3.1.3 Opportunities 203
6.3.1.4 Threats 204
6.3.2 Can We Hold Their Assets at Risk? 204
6.3.2.1 Strengths 204
6.3.2.2 Weaknesses 204
6.3.2.3 Opportunities 205
6.3.2.4 Threats 206
6.4 Can We Do So Repeatedly? 206
6.4.1.1 Strengths 206
6.4.1.2 Weaknesses 206
6.4.1.3 Opportunities 207
6.4.1.4 Threats 207
6.4.2 If Retaliation Does Not Deter, Can It At Least Disarm? 207
6.4.2.1 Strengths 207
6.4.2.2 Weaknesses 207
6.4.2.3 Opportunities 208
6.4.2.4 Threats 208
6.4.3 Will Third Parties Join the Fight? 208
6.4.3.1 Strengths 208
6.4.3.2 Weaknesses 208
6.4.3.3 Opportunities 209
6.4.3.4 Threats 209
6.4.4 Does Retaliation Send the Right Message to Our Own Side? 209
6.4.4.1 Strengths 209
6.4.4.2 Weaknesses 210
6.4.4.3 Opportunities 210
6.4.4.4 Threats 210
6.4.5 Do We Have a Threshold for Response? 211
6.4.5.1 Strengths 211
6.4.5.2 Weaknesses 211
6.4.5.3 Opportunities 211
6.4.5.4 Threats 212
6.4.6 Can We Avoid Escalation? 212
6.4.6.1 Strengths 212
6.4.6.2 Weaknesses 212
6.4.6.3 Opportunities 213
6.4.6.4 Threats 213
6.4.7 What If the Attacker Has Little Worth Hitting? 213
6.4.7.1 Strengths 213
6.4.7.2 Weaknesses 214
6.4.7.3 Opportunities 214
6.4.7.4 Threats 214
6.5 Suggestions for Future Research 214

6.6 Concluding Statements (and Future of China–Australia Cyber Relations) 215
References 217

List of Figures

Figure 6.1: Deterrence Model 194

List of Abbreviations

ACSC	Australian Cyber Security Centre
ADF	Australian Defence Force
AFP	Australian Federal Police
AI	Artificial intelligence
ANZUS	Australia, New Zealand and United States
API	Application programming interface
APT	Advanced persistent threat
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
AUKUS	Australia, the United Kingdom and the United States
CCP	Chinese Communist Party
CERT	Computer Emergency Response Team
CMC	Central Military Commission
CNE	Computer network espionage
CSOC	Cyber Security Operations Centre
DDoS	Distributed denial-of-service
DFAT	Department of Foreign Affairs and Trade
DSD	Defence Signals Directorate
DWP	Defence White Paper
GSD	General Staff Department

IT	Information technology
IWD	Information Warfare Division
MAD	Mutually assured destruction
MSS	Ministry of State Security
NATO	North Atlantic Treaty Organization
NII	National Information Infrastructure
NSA	National Security Agency
PLA	People’s Liberation Army
REDSPICE	Resilience, Effects, Space, Intelligence, Cyber and Enablers
RMA	Revolution in military affairs
SMS	Science of Military Strategy
SOCI Act	Security of Critical Infrastructure Act 2018 Act
SSF	Strategic Support Force
SWOT	Strengths, weakness, opportunities and threats
UK	United Kingdom
US	United States
UN	United Nations

Chapter 1: Introduction

This thesis will primarily examine the merits of cyber-deterrence approaches to influence an adversary's behaviour, with a focus on punishment strategies informed by Martin Libicki's (2009) framework constructed in *Cyberdeterrence and Cyberwar*. This framework will be applied to the Australia–China case study from the Australian perspective with the intention of assisting Australian decision-makers to ensure the achievement of Australia's strategic objectives in, and through, the cyber domain.

Such deterrence strategies and designs in cyberwarfare have transitioned from a niche, potentially unworkable or highly limited component of statecraft to an increasingly investigated, pertinent and implemented strategic mechanism to support Australian national interests (see Wilner, 2019). In addition, the 2023 Defence Strategic Review also recast Australia's defence mission by asserting that the Indo-Pacific has become the scene of 'major power strategic competition, the intensity of which should be seen as the defining feature of our region and time' (Department of Defence, 2023, p. 17), and it explicitly named China nine times. Given this backdrop, China has also been cited as responsible for more than two-thirds of state-sponsored cyber attacks worldwide as the cyber realm has become a new 'battleground' in state-to-state hostilities (Galloway, 2021). The scene has moved past being set and is now steadily transitioning to a state of strategic competition. Hence, deterrence measures should be investigated by Australian entities for attempting to stave off escalation.

Understanding deterrence approaches in cyberspace does remain a complex, multifaceted policy problem. However, in broad terms, cybersecurity can be regarded as an integral part of a country's strike as well as deterrence capability in both peacetime and wartime. In this sense, China's aggressive actions in cyberspace can be seen as short of traditional thresholds for war—although risks of escalation do remain. Nevertheless, from a deliberate Australian policy angle, deterrence itself has two basic components in the cyber realm that will generally fall below a level of armed or kinetic conflict: punishment or denial methods in efforts to secure and protect cyber ecosystems.

In exploring Australia's cyberwarfare requirements and challenges, deterrence by punishment refers to inflicting unacceptable costs on the attacker to influence their strategic decision-making (Mazarr, 2018, p. 4). In contrast, denial refers to efforts to protect against an adversary's attempt to attack (Mazarr, 2018). Australia continues to work across the full

spectrum of cyber-deterrence operations, and punishment and denial elements will both continue to be applied to its cybersecurity and defence frameworks, often set in a 'whole-of-government' context. Australia is also shifting towards more public displays of deterrence by punishment in dealing with attacks in cyberspace, including by boosting the offensive cyber capabilities of the Australian Signals Directorate (ASD), as will be explored in more detail in this thesis. However, in short, these punishment methods are driven by a cost–benefit analysis and the threat of a credible cost imposition.

The distinction between punishment and denial also has political and practical implications. As Denning (2015) asserted, part of the policy problem is that decision-makers have too often approached deterrence in cyberspace as a whole, all-encompassing security entity, rather than appreciating the opacity of cyberspace and addressing specific items such as force structure, adversary motivations, ambiguities of attribution, defence capabilities and the unique nature of different technological weapons or components.

Inferred in this argument is the cyber domain's place in a nation's strategy and how states such as Australia can apply national power for attempting to improve their relationship with another state (Layton, 2023). For Australia, in 2023 and beyond, this application of national power is shaping into a balance-of-power strategy (Layton, 2023). This strategy, 'underwritten by a military capability' will be potent enough to 'deter aggression and coercion' in the interest of a 'strategic equilibrium' (Wong, 2023). It is a strategy of deterrence focused at the great power level, incorporating, if not centralising, Australian allies such as the United States (US) and is directed at states such as China that may be destabilising the balance of power in Australia's geo-strategic areas of interest, including in the Indo-Pacific region (Layton, 2023).

The speed of development in the cyber realm does make it problematic to forecast and accurately predict what the realm will develop into. The proliferation of new and evolving cyber weapons and cyber tactics and a lack of understanding of the effects and implications of these contexts has been a significant issue facing decision-makers, resulting in some policy confusion and policymakers at times regarding cyber capabilities and associated 'weapons' as fantastical or frivolous (Leuprecht, Szeman & Skillicorn, 2019). At the very least, the ASD declaring that it will consider the use of offensive cyber capabilities to deter and respond to serious cyber incidents against Australia does remain highly controversial in efforts to deter China and other actors (Turnbull, 2017).

Compounding issues based on the strengthening cyberwarfare technical capability and related policy positions is the fact that cyber-deterrence practices will repeatedly outpace or overtake cyber-deterrence theory. As Wilner (2019) asserted, 'tactics, strategy, doctrine, and policy are developed and put to use even before corresponding theories are properly understood' (p. 245). Others such as Goodman (2010) have claimed that cyber deterrence proves 'easier in practice than it seems to be in theory because cyber-attacks are ultimately inseparable from the physical domain, where deterrence has a long-demonstrated record of success' (p. 102). Goodman (2010) also added that a critical lack of case studies has created debate over 'the efficacy of cyber deterrence' (p. 103). This is despite cyber-deterrence debate points often being incorporated into an extensive knowledge platform that has emerged from traditional deterrence theory.

In this sense, the cyber realm is, and should be, seen as a distinctive reference point and as constituting a unique fifth domain in which wars can be fought—alongside air, land, sea and space. Moreover, cyberspace will continue to pose distinctive challenges for policymakers and strategists (Cybersecurity and Infrastructure Security Agency, 2023, p. 2). Thus, in addressing the effectiveness of cybersecurity, risk management issues and related deterrence frameworks, parallel to the advancing digitalisation of ever more aspects of the economy, society and politics, cybersecurity concerns are expanding to additional policy domains and cybersecurity is simultaneously moving upwards in the political agenda and expanding sideways as a problem area to include a multitude of additional policy domains (Cavelty & Wenger, 2020).

Overall, the current global connectivity and advancing digitalisation pose various defence challenges and ongoing security threats for Australia. Cybersecurity discourse has also come to the forefront in the national political and defence thinking. Thus, a seminal problem that this thesis will investigate is the efficacy of cyber deterrence and the assumptions surrounding the applicability, effectiveness and credibility of deterrence, particularly punishment, within the cyber domain. This will be illustrated through an Australia–China case study and the risks implied by a rising competition with China.

Certainly, there are legitimate concerns about the efficacy of cyber deterrence. The concept of deterrence indicates 'a form of preventive influence that rests primarily on negative incentives' (Paul, Morgan, & Wirtz, 2009, p. 2). A key scholar who has described cyberwarfare and has attempted to align the concept of deterrence theory to cyber deterrence against a cyber-attack war is Martin Libicki. He is an adjunct management scientist at the RAND Corporation and a

Distinguished Visiting Professor at the US Naval Academy. He has addressed various facets of cyber attacks for more than a decade and considers cyberspace as an 'operational domain' in defence and security terms. Libicki (2018) has asked the important policy question of whether states (in this case, the US) should 'emphasize the possibility by impressing adversaries with what cyber-attacks can do, reminding adversaries that the United States would be willing to do it, and investing in making cyber-attacks more reliable and even more painful' (p. 44).

Libicki (2017) has also argued that a successful posture of deterrence—that is, the use of threats to compel others to restrain themselves—must have certain prerequisites including that of being able to correctly attribute cyber attacks in order to punish the correct party and convince others that the punishment is justified as well as the need to have and communicate thresholds—namely, policy actions that will or might lead to reprisals. This was informed by Libicki's 2009 study that established the nine-question framework investigated in this thesis (pp. xvi–xviii).

As explored in more detail below, this thesis will therefore address the efficiency of cyber deterrence by utilising Libicki's investigative framework but will apply it to the operational and associated realities of an Australia–China context (and still primarily state-on-state contests). This template aims to address the gap between theory and practice while laying out a lucid, valid decision matrix that will both support and explore the logic of deterrence and the connection points between attack and retaliation in the cyber realm. Overall, Libicki presented a comprehensive understanding of cybersecurity and cyber deterrence to facilitate a better understanding of the policies, operations and strategies of various defence and security sectors, and such carefully calibrated framing continues to remain highly relevant to decision-making for Australia in the context of its interactions with China.

Furthermore, while cyber operations can have significant policy opportunity costs and benefits, cyberspace itself remains

> a thing of contrasts: It is a space and is thus similar to such other media of contention as the land and sea. It is also a space unlike any other, making it dissimilar. Cyberspace has to be appreciated on its own merits; it is a man-made construct. Only after coming to such an appreciation is it possible to pick through what we believe we know about deterrence, physical warfare, and warfare in other media to figure out which elements apply in cyberspace and to what extent. (Libicki, 2009, p. 11)

1.1 Research Aims, Context, Methodology and Objectives

How challenging and intricate is cyber deterrence in the backdrop of the Australia–China relationship?

As a starting point, Libicki (2009) defined cyberspace as 'the agglomeration of computing devices that are networked to one another and to the outside world' (p. 6). He also differentiates between two types of cyberwar. The first is a strategic cyberwar, in which cyber attacks are 'launched by one entity against a state and its society primarily but not exclusively for the purpose of affecting the target states' behaviour' (Libicki, 2009, p. 117). In contrast, the second type, an operational cyberwar, is 'the use of a computer network to support physical military operations' (Libicki, 2009, p. 117).

As aforementioned, deterrence by punishment is a subset of coercion—the threat of force to persuade a potential state-based aggressor that the value of a certain cyber action is outweighed by the expected punishment. Simultaneously, any state actor must also ensure that it succeeds in the signalling or communication of its capability and competency, such as the threat of retaliation to the potential aggressor (see Paul et al., 2009, p. 2). Further, as Morgan (2010) revealed, deterrence 'is a psychological relationship; the goal is to shape an opponent's perceptions, expectations, and ultimately its decisions about launching an attack' (p. 56). In short, a central question regarding the strategy of deterrence by punishment concerns the conditions under which it is likely to be 'successful' in causing a potential adversary to avoid or forestall challenging a particular target or the defender.

Therefore, in terms of an Australian context, the thesis objective is to address and evaluate particular assumptions related to:

1. the possibility of accelerated cyber conflict and cyber competition between Australia and China,
2. the meaning of cyberwarfare in an ever-evolving threat landscape,
3. the merits of cyber deterrence based on the magnitude of the cyberthreat attributed to specific state actors,
4. the context of Australian and Chinese strategic cyberwar and related capabilities and developments, and

5. the application of deterrence-by-denial and deterrence-by-punishment strategies in order to determine their applicability and value for future policymakers.

As Australia's position is increasingly being tested by China's cyber attacks, the principal research question is:

- Is Cyber Deterrence by Punishment possible?

The interrelated secondary questions are:

1. What is the nature of threat to Australia posed by China in the cyber domain?
2. What are the main challenges for Australia in ensuring an effective, credible utilisation of a deterrence-by-punishment strategy?
3. Given the rapidly changing dynamics of cybersecurity and related information technologies (IT), what is the best policy path in the direction of the cyber-deterrence discourse, escalation dilemmas and related defence policy from an Australian perspective?

Therefore, in efforts to establish a reasonable set of answers that could inform the role and impact of cyber deterrence as a course of action for Australian policymakers to deal with China, the thesis is structured as follows.

Chapter 1, the introductory chapter, will describe key concepts and terms, including cyber deterrence and cyberwar. It will also present a literature review detailing a broad analysis of cybersecurity issues and a review of deterrence theory and strategy to facilitate a discussion later on the applicability of deterrence frameworks in the cyber domain, including deterrence by denial as a passive strategy and deterrence by punishment as an active strategy.

Chapter 2 will address the history and backdrop of Australia's cybersecurity thinking. It will incorporate an analysis of various official white papers and related secondary material that have aimed to act as a 'roadmap' for the Australian Government's pursuit of cybersecurity and the establishment and projection of its cyberwarfare capabilities. Significantly, the Australian government has expanded the definition of cyber deterrence to allow the option to confront adversaries offensively and to signal penalty measures for attacking Australians' core critical infrastructure.

Chapter 3 will unpack China's cyber capabilities and the development of its cyberwarfare policy, specifically military development and associated cyber units that are confirmed to be tied to its government. Thus, the thesis will also address groupings known to engage in cyber attacks called advanced persistent threats (APTs) that make significant cyber intrusions globally and have been identified and linked to the Chinese Government or operating within China. Chapter 3 will also present an analysis of possible Chinese escalation thresholds based on China's official policy—or at least state whether it is unclear—and weigh the risks of violating said thresholds against operational necessity in Chapter 5. At the very least, there is a level of political intelligence needed in order to understand the motives and capabilities of an attacker such as China—including its doctrine for cyber deception—that can allow the development of appropriate policy commitment and organisational capacity.

Chapter 4 will explore the question of whether attribution is possible. Attribution remains a significant issue for all actors in the cyber domain in aligning offensive actions and deterrence capabilities. The chapter will analyse the difficulties in carrying out attribution, the political and strategic complications in attributing cyber attacks and the attribution methods that states may employ. It will also review the offensive tools widely available in cyberwarfare that could facilitate deterrence by punishment. This chapter is essential to contextualise actions that are actually possible in cyber deterrence in order to provide a cohesive structure to policy and strategic considerations.

Chapter 5 will analyse and discuss the capability and applicability of cyber-deterrence mechanisms and possible pathways for the Australian Government policy to address the challenge of China through the lens of deterrence by punishment. The chapter will focus on the defender's (Australia) capabilities, the credibility of the threat and the ability to relay a cogent, effect threat message to China. Further, the chapter will break down Libicki's questions by referring to the context and analysis provided in prior chapters, including key issues such as the credibility of the threat and the relaying of the threat message to the adversary. In summary, while Australia has adeptly increased its national cyber capabilities, it needs to implement more changes to maintain resilience, effectiveness and flexibility in its cyber-deterrence options.

Chapter 6 will address policy implications for Australia via a strengths, weakness, opportunities and threats (SWOT) analysis (see below) and will summarise the suitability of cyber-deterrence frameworks to provide a cogent, effective deterrence agenda and context. This concluding chapter will also unpack how deterrent strategies should be fortified as much

as possible via defensive capabilities to deny China success and benefits from attempted escalation.

Overall, this thesis concludes that Australia has a strong foundation for deterrence progress. The SWOT analysis will be based, in part, on the assessments about Australia's cyber capabilities and related policy vis-a-vis China and implications of the deterrence postures that have been explored in Chapters 2, 3, 4 and 5.

Studies on threats in cyberspace should be refined and value added to these. In recognising the complex, problematical nature of cyber deterrence, Libicki (2009) proposed a template or blueprint for policy responses in order to, in part, explore 'less-risky or less-harmful options to achieve a relative degree of peace in cyberspace' (p. 91). While many considerations about the logic of deterrence by Libicki are based on a US perspective and 'one size does not fit all' in comparative study, his analysis and framing do continue to have strong relevancy and value from an Australian standpoint as well. Libicki's template does allow for various lines of inquiry about cyber-deterrence requirements, capabilities and challenges in a scenario in which Australian policymakers and allied others continue to find various interrelated modern-day policy debate points (including the connection between attack and retaliation) contested and controversial (see Egloff, 2020b; Moulin, 2023).

For instance, with a focus on state actions, Moulin (2023) argued that if a given cyber attack

> is wrongful and a state was behind the operation, then attribution is possible from a legal point of view (legal dimension). However, attribution is also a sovereign political decision which is adopted with due consideration for the broader context (political dimension). (p. 74)

It is also this political dimension in which deterrence by punishment will be contemplated, and again, Libicki's (2009) template allows such policy formation, risk assessment and mitigation strategies that focus on both threat prevention and detection.

Nevertheless, in short, cyber deterrence is still the subject of much uncertainty. Other ongoing policy difficulties for Australia include issues related to attribution, asymmetry and a lack of clarity in the field. As explored later, for instance, Australia has mooted its modern-day offensive cyber capability, but many details under Project REDSPICE ('Resilience, Effects, Defence, Space, Intelligence, Cyber and Enablers') remain unclear, while

> offensive cyber operations carry several risks that need to be carefully considered. For cyber operations in support of the ADF [Australian Defence Force], as with conventional capabilities, the commander must weigh up the potential for achieving operational goals against the risk of collateral effects and damage. (Hanson & Uren, 2018, p. 8)

Moreover, Australia has argued that the threshold for public attribution on a technical level is extremely high.

Further, both Australian and US conceptions of deterrence identify the importance of cyber stability that can be achieved through cyber-deterrence positioning. Moreover, in 2011, it was announced that the trilateral *Australia, New Zealand and United States Security Treaty, 1951*, (ANZUS Treaty) would be extended into cyberspace. It had also been contemplated as early as 2012 that 'the intended recipient of any intended message is presumably China, and the message is that cyber-attacks, while perhaps falling short of the seriousness of armed attack, are unacceptable and may attract a serious response' (Davies, Lewis, Herrera-Flanagan, & Mulvenon, 2012, p. 29).

Thus, against this background, Libicki (2009) sets out a deterrence menu consisting of nine main questions:

1. Do we know who did it?
2. Can we hold their assets at risk?
3. Can we do so repeatedly?
4. If retaliation does not deter, can it at least disarm?
5. Will third parties join the fight?
6. Does retaliation send the right message to our own side?
7. Do we have a threshold for response?
8. Can we avoid escalation?
9. What if the attacker has little worth hitting? (p. 39)

As Australia shifts to a new security mindset aimed, in part, at defending against adversaries in cyberspace, the impact and importance of such of cyber-deterrence framing is especially applicable, with an emphasis on questions 1, 5, 6, 7, 8 and 9. These six are particularly relevant in the Australia–China context, given that these fit into a crisis-management spectrum and the ongoing need and importance of not creating an accidental or counterproductive escalation of tensions associated with a major cyber attack. The assumption is that Australia currently aims

to construct robust cyber defences while avoiding the creation of an international crisis and of incentives for China to be drawn into a spiralling pattern of strategic instability with Australia.

Further, Australia has repeatedly called on particular countries, including China, to act responsibly in cyberspace. Yet, cyber attacks against Australia from state-sponsored (and criminal) groups skyrocketed in 2021 and 2022, and government report estimated that there was one attack every seven minutes (Australian Cyber Security Centre [ACSC], 2022a). Similarly, in 2023, Australia joined other Five Eyes partners in outing China as being behind a cluster of cyber attacks that had targeted critical infrastructure in the US. America, Britain, Canada and New Zealand issued a joint advisory statement with Australia that said it was believed China would apply the same techniques against other sectors worldwide (Australian Signals Directorate, 2023).

Hence, this thesis aims to integrate Libicki's (2009) nine broad-based, general exploratory questions into an explicit context, namely, the Australia–China relationship, to better understand cyber stability and associated crisis dynamics in cyberspace across a deliberate geopolitical and cyberspace context. As noted, China is widely believed to be behind a continuing range of hacking and related attacks on Australia's cyber infrastructure. China itself also did not have an official cybersecurity policy until 2006 (Miao & Lei, 2016). However, at the very least, the advance of cyber capabilities does open up nonlethal options for policymakers, which are considered less threatening than traditional weapons with kinetic effects. One associated purpose of the case study is to help understand the requirements for discouraging cyberwar between Australia and China and to identify the likely elements of a credible, effective deterrence relationship.

Importantly the Libicki questions do have an enduring applicability to address cyber conflict from an Australian perspective as well as to explore the often poorly understood nature and role of cyber deterrence. The answers to these questions will need to address the 'attribution problem', the application and potential escalation of cyber attacks, whether the intrusion/conflict should become public knowledge, standards to investigate 'red lines' and related deterrence thresholds and whether existing cyber capabilities can act as effective means of coercion. For instance, a fundamental starting-point policy problem is that the capacity to punish cannot be present if attribution is vague or missing. Simultaneously, the testing or trial of related capabilities could potentially increase the chances of miscalculation and mistake.

Overall, Libicki has provided a facilitating agenda and itemised structure that can guide the investigation in this thesis of whether deterrence strategies can effectively and credibly work in the cyber domain, albeit utilising Australia and China as topics of a necessitated case study (2009). In practice, each of the question components will be linked to, and addressed in, certain chapters, with Chapter 5 addressing the framework in its entirety and Chapter 6 via the aforementioned SWOT analysis, as shown in the following table:

Question	Chapter
1	3, 4, 5
2	5,
3	5,
4	5,
5	3, 4, 5
6	5,
7	2, 5,
8	4, 5,
9	3, 5, 6

Cyberspace and the above questions certainly continue to pose unique challenges for decision-makers. Goodman (2010) highlights that any cyber-deterrence framework will differ from traditional military and defence frameworks, especially nuclear frameworks, as the potential damage and various other crisis factors are simply not as dire or existential in the cyber domain as in the nuclear one (p. 127). Yet, Goodman (2010) has also argued that treating cyber deterrence as only theoretically possible—that is, ignoring the geopolitical context in which cyber attacks occur—can unintentionally underestimate its application and potency and exaggerate its difficulty (p. 102).

At the very least, cyber deterrence and cyberspace do remain associated and even coupled to tangible physical and active political worlds. In this instance, such an assessment will incorporate the undercurrents between Australia and China to illuminate and evaluate cyber-deterrence challenges, including those associated with managing the risk of accidental or inadvertent escalation as an interactive phenomenon.

Thus, it is hoped that employing and applying Libicki's (2009) template will assist in the development of robust policy foundations for a cyber-deterrence strategy in Australia that identifies the type of tailored, context-sensitive deterrence posture and related approaches that will be the most effective to advance Australian interests. As Goodman (2010) stated, while cyberspace 'does pose unique challenges for deterrence strategists, real-world cases demonstrate that those challenges can be overcome' (p. 128). Further, from a policy-centric perspective, the thesis hopes to reduce the divide between policymakers and those invested in the more technological and IT dimensions of cyberspace in efforts to address the core requirements of cyber deterrence.

Last, the relationship between China and Australia as a case study will be the context of analysis within all chapters and will act as a consistent reference point for examining digital military arsenals. As C Williams (2021) noted, 'the threat posed by Chinese cyber-attacks in Australia is not new, but the scale of activity is becoming of greater concern'.

The significant levels of interaction between the two nations in the cyber domain, both public and private, provides a rich, in-depth source of data, especially data on strategic cyberwarfare operations (Austin, 2016a). Case study research 'aims to explore and depict a setting with a view to advancing understanding of it' (Cousin, 2005 p. 421). 'In general, case studies are the preferred research method when "how" or "why" questions are being posed' (Yin, 2003, p. 10). Case study research is useful as it constantly considers the context of said case: 'a case study is an empirical inquiry that investigates a contemporary phenomenon (the "case") in depth and within its real-world context, especially when the boundaries between the phenomenon and context may not be clearly evident' (Yin, 2014, p. 16).

Case studies are advantageous in establishing a strong, practical framework using which the research can then be conducted, thus ensuring focus and a cogent analysis. Therefore, an Australia–China case study is well suited to the research questions explored in this thesis, and the utilisation of the case study method allows the use of an adaptive, instrumental approach. This approach facilitates a more nuanced investigation of the data and the presentation of more detailed SWOT-analysis-based policy recommendations in Chapter 6.

1.2 Background

An initial issue, given a host of new cyberthreats that require constant attention, is determining the point at which a cyber-espionage operation becomes or can be viewed as a deliberate cyber attack—or labelled as a ‘cyberwar’. There are several elements to consider in this regard because, in part, deterrence involves considering the conditions under which it is likely to be successful. In certain circumstances, cyberwarfare and cyber-espionage activities can be combined, and deterrence concepts may also aim to prevent or mitigate different types of cyberthreats.

For the purposes of this thesis, the ACSC (2020) definition of a cyber attack will be employed: ‘A deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computer or networks, the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity’. The ACSC itself can be seen as a critical focal point for protecting infrastructure as well as private and public sector cooperation and information sharing on improving cybersecurity in Australia.

This definition also commonly describes a politically motivated attack with malicious intent, whereas the term cybercrime most often describes activity for purely criminal ends. Nevertheless, motives behind attacks can be difficult to determine. For example, Ryuk is a ransomware attack that exploits vulnerabilities in computer systems and networks, and while this type of attack has been deployed numerous times across the world, it has also been used as a case study for unpacking the ACSC definition (see Jenkinson, 2020). Ransomware holds computers or files hostage by encrypting the data and withholding the access details from the legitimate user. It is launched using multiple tools.

First, a ‘phishing’ email is sent to potential victims, in the hope that the receiver will click on malicious links in it. If the link is clicked, the Emotet Trojan malware is downloaded onto the computer. The attacker gains entry. Once this occurs, Emotet deploys TrickBot, whose purpose is to examine the victim system for potentially rewarding datasets. If the attackers hit a government network, then the Ryuk ransomware will be deployed across that network, and it encrypts files and denies users access until, typically, they pay a ransom for the password to this ransomware.

Such an attack has important connotations that are especially significant for deterrence. The deployment of Emotet itself is not a cyber attack, but it is, and should be viewed as, espionage. As discussed in Chapter 2, the Australian Government or at least its entities not only accept that cyber espionage—the theft of Australian information or capabilities for economic gain, competitive advantage or political reasons—occurs and has grown considerably in cyberspace but also that Australia also attempts to glean such information from its adversaries (Noble, 2020).

However, the important words in the ACSC definition are the 'deny and disrupt' components—only the Ryuk ransomware actually denies or disrupts the use of computers or networks. At first, the definition appears convoluted, but in a practical sense, it is useful in preparing for and responding to cyber incidents. Therefore, whenever a cyber attack is referenced in this thesis, unless strictly stated otherwise, it refers to a cyber operation that manipulates, disrupts, denies, degrades or destroys computers. A set of ransomware attacks per se will naturally not reach the threshold for cyberwar. A cyber-espionage action in itself also might not alter networks themselves in a way that changes or alters their current or future ability to function, particularly as in many instances of network penetration the attacker is conducting surveillance before anything else (Westbrook, 2017).

Nonetheless, the cyber domain is becoming increasingly relevant as a new arena of strategic contest (Sear, 2019). According to Libicki (2009), strategic cyberwar is a campaign of cyber attacks that one entity carries out on another, which may be unilateral. However, for this discussion, it shall be assumed it is mainly between two sides—Australia and China as the prime antagonists—and this thesis explores the likely events when attack, retaliation and counter-retaliation degenerate into continual conflict beginning in the cyber domain, which may or may not spill out into the physical one (Libicki, 2009, p. 8).

In addition, Freedman (2004) discussed 'immediate' versus 'general' deterrence, distinguishing between a crisis situation between known actors against unknown or would-be aggressors. In this instance, such investigative elements regarding attacks through cyber means, given that the case study is China, will therefore fall into the 'immediate' status.

Overall, in light of the benefits inherent within deterrence aimed at reducing the scope of competition to spill over into kinetic violence, it is this method of cyberwarfare that the thesis will primarily investigate—as it is most closely related to the intended strategic effects of

deterrence. In summary, cyberwar ‘is undertaken to affect the will of the adversary directly (it can also be considered tantamount to strategic cyber war)’ (Libicki, 2014, p. 29). Yet Libicki (2014) also cautioned that ‘there is the possibility that the strategic effects of cyber war may arise from the interaction of state actors that systematically overestimate its effects’ (p. 33).

1.3 Significance

Cyber attacks are a serious threat to Australian national security, and their context as well as interpretation will affect future deterrence ideas, crisis management and security interactions. A key contribution of this thesis is in the development of a holistic, feasible deterrence strategy in cyberspace and the avoidance of hyperbole in explaining new forms of conflict.

Perhaps Major General Marcus Thompson (retired), who was Head of Information Warfare for the Australian Defence Force (ADF), stated it most simply in 2019—there is not cyberwarfare, there is just warfare (as cited in Stilgherrian, 2019). The implication of this statement is that the act of warfare itself is multifaceted, and warfare is spreading away from traditional domains as systems become more networked and the possibility of cyber attacks escalate. Cyber attacks might aim for a wide range of disruptive outcomes, given that societies have become more digitised, supply chains have become transnational and the stability of cyberspace systems remains crucial in facilitating productive output and activity in order to accomplish a wide range of national goals.

Owing to loopholes and vulnerabilities, these networks and web resources that store personal and private information can be exploited and weaponised by actors seeking a crucial leverage and advantage or seeking to cause harm and disruption with either criminal or even terroristic implications (Brenner, 2007). As noted, China has routinely been accused by various nations, including Australia, of cyber attacks (and cyber espionage), which have had a negative impact on crucial modernised services and IT systems (Besser & Sturner, 2016). For instance, a 2016 Defence White Paper (DWP) highlighted the ‘complex non-geographic threats’ in cyberspace and how various capabilities and platforms could be adversely affected (Department of Defence, 2016, p. 16). Hence, there is the possibility of a cybersecurity dilemma spiralling out of control.

For example, the Australian Government revealed in 2019 that a foreign power had hacked the email servers every major political party at the federal level and that China was the prime

suspect (Wroe, 2019). This particular attack was significant in that the ASD labelled it the first official cyber crisis (Dillon, 2019). The hits on government computer networks and the cyber violation of the Liberal, Labor and National parties revealed many significant aspects of the problem of cyber intrusions.

First, cyber intrusions are insidious in nature for these are often deliberately secretive and aspire to ensure the attacker is hidden for as long as it takes to acquire crucial data. Consequently, the extent of time that elapses between the observation or discovery of a vulnerability and the implementation of suitable deterrence actions can vary widely. Second, no data or related target appears to be off-limits—if it is networked, then actors will attempt to penetrate the target network and extract data with various effects. Third, attributing these sorts of attacks in any network and making a deliberate and accurate accusation of cyber intrusions is difficult both technically and politically but not impossible (Sadler, 2019). However, any deterrent strategy should attempt to prevent a conflict from escalating to the use of kinetic force. Of course, punishment might also not be leveraged exclusively through the use of cyberspace; other instruments of power and leverage might involve diplomatic and/or economic means.

Thus, decision-makers may need assistance in *how* to respond. Austin (2016b) reasoned that states seeking to deter an adversary must show that they have the capabilities and intent to follow through, and Australia would need 'to develop complex responsive systems of decision-making for medium intensity war that address multi-vector, multi-front and multi-theatre attacks in cyber-space, including against civilian infrastructure and civilians involved in the war effort'. The development of a threshold or the elaboration of criteria, regarding acts that would constitute an 'unacceptable' cyber attack that would trigger an official response, might also be necessary.

Nevertheless, any actor seeking to deter must reveal, at the very least, that it has the capabilities to deny the adversary its objectives and to launch an effective counterstrike (Sear, 2019). In other words, without comprehensive capabilities to identify they have been attacked and then to attribute the attack successfully to the purported attacker, all states will struggle to craft effective deterrent mechanisms to hinder the proliferation of such attacks. Building cyber deterrence will require a comprehensive approach to cybersecurity, and as Australia and China's relationship grows more intertwined, any framework of deterrence will need to not only be effective but also aim to not cause significant or unforeseen escalation (Solomon, 2019).

Further, there is a trend to compare kinetic or nuclear deterrence with cyber deterrence. Therefore, this thesis will focus on various types of deterrence aligned to the overall framework provided by Libicki and incorporate discussions on problems such as proportionality. In addition, critical national strategy papers and announcements, such as DWP 2016, did announce the Australian Government's intention to vastly increase its capability to ensure a secure internet for Australians across the spectrum of business, social and defence interests, and importantly, granting 'round the clock' operations for the ASD and Australian Computer Emergency Response Team's (CERT). The identification of the common factors in these strategies, bodies and policy declarations completes the ambit of the investigation in this thesis of the possible deterrence options available to Australia which will then be applied to actors such as China.

Thus, in general terms, the investigation of deterrence strategy in the cyber domain is significant as a contribution to the security discourse on an increasingly important aspect of both public and private interests. In Martin Libicki's (2009) *Cyberdeterrence and Cyberwar*, he posited:

> Cyberspace is its own medium with its own rules … The medium is fraught with ambiguities about who attacked who and why, about what they achieved and can they do so again … Thus, deterrence and warfighting tenets established in other media do not necessarily translate reliably into cyberspace. Such tenets must be rethought. This monograph is an attempt to start this rethinking. (p. iii)

This thesis will also further this mode of rethinking through an Australian perspective against a powerful aggressor such as China. As Libicki (2011) suggested, various military and security sector analysts had been debating how to maintain a strategic advantage in cyberspace (p. 72). Governments around the globe continue to seek to attain this advantage by establishing various specialist cyber-operation centres, such as the Cyber Command in the US, or the ACSC that began operations in 2014 in Australia to respond to cybersecurity threats and incidents. In 2018, the ACSC expanded and formally became part of ASD (ASD, 2023). The establishment and growth of such centres, the development of capability and the announcements from various government figures all promote the continued importance of preventing and combatting threats and minimising harm in the cyber domain.

Last, the cyber domain must be understood in its own terms—it is an incredibility distinctive domain in discussions on cyber strategy and cyber deterrence. Again, this fact has led to

extensive, fluid speculation on the types of cyber attacks and associated effects that would constitute the crossing of a ‘red line’ that would justify going to war (Nevill, 2015). As Van de Velde (2023) asserted:

> Because cyberspace is the lifeblood for all domains, it cannot be a source of vulnerability to DOD (Department of Defence) operations. Hardened networks that effectively resist attack and exploitation can impose greater costs on would-be adversaries. Resilient networks, designed to operate in degraded states, are prerequisites for deterrence and will promote the idea of futility in the mind of potential adversaries. (p. 49)

This view remains highly pertinent in debate points about defence capabilities, political willpower and fortitude and the prerequisites for effective deterrence through cyberspace.

1.4 Limitations

One of the most significant limitations in cyberwarfare is its secrecy and its often classified nature. Individuals such as former US Director of National Intelligence James Clapper (2017) have stated that the excessive secrecy of the cyber domain is a limiting factor for observers to debate how to best provide credible and effective cyber-deterrence capabilities. Libicki (2009) mentioned the viability of *sub rosa* communications between adversary states, such as Australia and China, but a limitation for public consideration is the inherent secrecy of these communications. Before even considering the secrecy of the technologies being deployed, the communication aspect is already potentially murky, which is a problem for the communicative element of deterrence by punishment.

For example, at the time of writing, the precise threshold (Libicki’s question 7) for an armed response to a cyber attack was not clear-cut, and nor has it been publicly discussed by Australian (or US, for that matter) policymakers. Another example would be various controversial aspects tied to the use and goals of defence and security. The Australian Government’s REDSPICE project, announced in 2022 and discussed further in Chapter 2, pledged to increase both protective and offensive cyber capabilities as part of Australia’s cyber-deterrence posture. However, whether

> Australia should use offensive cyber capabilities against other actors and, if so, against who, remains highly contentious. This ambitious project has raised many unanswered questions about what ‘offensive’ digital capabilities and ‘cyber-hunt activities’ might entail. There are

> potential ramifications with regard to domestic and international law, as well as the norms of good international behaviour. (Baldino, 2023)

Further, in broader terms and as pointed out by Hanson (2017), Australia's offensive cyber capability

> is an important new national security capability and a valuable addition to the ADF [Australian Defence Force]. While most of its work will remain a secret, a little more clarity around its broad role and objectives will help ensure a more informed debate about its utility and need. It will also help frame international standards of acceptable behaviour.

Even the location of the new high-security Cyber Security Operations Centre (CSOC) based in Sydney remains a classified secret, although it has been publicly announced to protect Australians from cyber attacks.

In such a context, Clapper's admission is especially significant, as it indicates that states must be willing to consider all their academic, workforce and associated talent in strategic and related considerations in order to fully utilise a nation's cyber capability and posture. Yet, despite such admissions, Australia continues to remain highly secretive about the technical capability of its cyber weapons, in particular; their precise composition and design; and the operational objectives of the teams that could deploy them—especially offensively.

Thus, this lack of open-source information limits the examination in thesis at both the operational and strategic level of analysis. Nevertheless, the analysis at the operational level may indicate general opportunities for improvement in the operations of cyber strategies and the strategic analysis will utilise the SWOT method—a method that is highly helpful in providing insights to innovate and develop advanced countermeasures against evolving cyberthreats. As a cautionary note about using a SWOT analysis to address such sensitive security issues, as highlighted by Blaxland (2019), critics may see this as excessively

> reductionist and constraining. Indeed, the SWOT methodology depends on being selective and inclusive of conceptually compatible components. Yet in order to gain a sense of scale and severity of the challenges faced, such categorisation and compartmentalisation is warranted. (p. 3)

As aforementioned, cyber-attack interpretations for this thesis will also follow Libicki's 2009 definition and will be based on state attacks on critical infrastructure and attacks on the defence

systems of other state actors. Such a framing is important in examining cyber attacks and cyber deterrence and is distinct from analysis that moves into the realm of cyber espionage and non-state criminal actors. The acts of penetrating networks and conducting surveillance, while not desirable from a sate victim standpoint, are not actions that would lead to the degradation or deliberate incapacitation of networks, systems or servers and therefore would not be suitable as a possible warfare operation. Neither would the pilfering of information, such as in the examples already discussed.

Libicki (2009) also stipulated variations on cyberwarfare itself, to avoid confusion with espionage activities. Thus, this thesis will, as already stated, focus on what he calls 'strategic cyberwar', which is a campaign launched by one state entity against another state and its society for the primary purpose of affecting that target state's behaviour (Libicki, 2009, p 117). Further, while a military campaign can be launched by a non-state entity, and not necessarily a state actor, Libicki (2009) often constrained his own investigation by narrowing it to state-on-state contests (p. 117). The focus of state actors in this thesis, specifically China, refers to a state actor that has posed or may pose a threat to Australia through cyber attacks.

Certainly, cyberthreats to Australia can be split into state or non-state threats. Non-state actors range from corporations engaging in economically motivated cyber espionage to criminal networks attempting to destroy or disrupt financial systems, insurgents engaging in online propaganda and falsification of information, and even lone individuals who can pose a significant threat to states. Hence, also owing to the extreme range of non-state actors, this thesis will not attempt to investigate deterrence strategies that may resolve these types of important issues since the scope of the thesis would be too large and unwieldy.

Concurrently, simply stating that the thesis will focus on state actors is also disingenuous—the investigation will be deliberately restricted to China and Australia to limit the analysis scope and provide a greater depth of analysis. Despite the acknowledgement of private and public threats in the cyber realm, this thesis will largely focus on the threats to states themselves. It will also not consider issues such as collective security or constructivist-driven practices, such as norms to which states can adhere with the idea that eventually this will lead to greater cooperation (Hurwitz, 2015). By strictly adhering to deterrence strategy, this thesis will analyse Australia's individual capacity to deter a greater power such as China. Therefore, despite the importance of cyberthreats to private institutions, this thesis will focus primarily on state-level cybersecurity.

The distinction between active and passive deterrence is important, and this thesis focuses primarily on active deterrence, or deterrence by punishment, rather than on deterrence by denial. Libicki (2009) stated that deterrence by denial is essential in the cyber domain and that it is, for the most part, more effective than deterrence by punishment however, ignoring deterrence by punishment offers nothing to strategists seeking to maximise the deterrence capabilities at their disposal, and that punishment and denial deterrence strategies are synergistic (2009, p. 8).

Regardless, this thesis acknowledges that states' deterrence strategies are weakened by not investigating all methods available, and that deterrence by punishment, if effective, can in fact enhance deterrence-by-denial methods as it essentially reduces the strain on denial-based solutions. Libicki (2009) positioned the framework as a deterrence-by-punishment tool not only in writing but also by the very questions he framed. For example, the three primary questions of the framework are (1) *Do we know who did it?* (2) *Can we hold their assets at risk?* (3) *Can we do so repeatedly?* (Libicki, 2009, pp. 41–56). In particular, questions 2 and 3 are offensive in nature and intended to cause potential adversaries harm, not prevent adversary nations from succeeding in their attacks.

Such limitations restrict the thesis to investigating ways to deter adversaries through risk assessments, passive deterrence and offensive punitive cyber measures against critical infrastructure that might offer strategic and signalling benefits to Australia.

1.5 Literature Review

Deterrence by punishment and denial by defence were central features of nuclear deterrence theory. In a Cold War environment, circumstances transpired whereby a state actor would attempt 'to prevail by making the other think it is going to stand firm' (Jervis, 1979, p. 192). Hence, extended deterrence required the US to maintain the credibility of any threat to kinetically attack the Soviet Union via massive nuclear retaliation.

Similarly, in a post-Cold-War setting, the deterrer must communicate the threat of massive retaliation to an adversary. Nonetheless, deterrence via denial alone is impracticable in the cyber domain. It is also non-kinetic. While the DWP 2016 openly stated that Australia remained committed to a rules-based global order as the best interest for attaining its strategic objectives, there 'is no international consensus on a precise definition of a use of force, in or

out of cyberspace' (Schmitt, 2011, p. 573). Moreover, in broad terms, substantial differences remain between nuclear deterrence and cyber deterrence:

> With nuclear deterrence, the United States must deter the single nuclear explosion. With cyber deterrence, the United States is managing an ongoing, constant problem and a spectrum of malicious activity from the small (influence operations) to the strategic (attacks on infrastructure). In the cyber realm, we cannot simply exercise or demonstrate our capabilities to the world at an airshow or weapons fair, and so we refrain from establishing clearly marked red lines, opting instead to lead by example, by not stealing proprietary information or attacking the critical infrastructure or key resources of another state. (Van de Velde, 2023, p. 43)

Therefore, in addressing deterrence theory, it is critical to emphasise the unique features of cyberspace as the domain becomes ever more important owing to the Internet of Things and related cyber-hygiene concerns among the populace and the increasing vulnerabilities and dependencies in the cyber realm of the military and corporate worlds. Yet, cyber-domain effects also certainly do not equate to the effects of a nuclear weapon. Thus, the analogy to nuclear deterrence can be highly misrepresentative and distorted. In exploring some of the ambiguities of cyberthreats from an American angle, Nye (2016) emphasised:

> In contrast, many aspects of cyber behavior are more like other behaviors, such as crime, that the United States tries (imperfectly) to deter. Preventing harm in cyberspace involves complex mechanisms such as threats of punishment, denial, entanglement, and norms. Moreover, even when punishment is used, deterrent threats need not be limited to cyber responses, and they may address general behavior as well as specific acts. (p. 45)

Consequently, integrated ideas about integrated deterrence should be seen as sometimes intending to expand the nuclear deterrence paradigms to encompass all deterrence regimes across all domains to, in part, allow improvements in capabilities. Nevertheless, unlike kinetic weapons, cyber operations remain asymmetric, precipitous, sometimes undetectable and characterised by an absence of physical devastation or loss of life. In cyberwarfare,

> attacks occur at nearly the speed of light. You get little warning or time to react. The initial strike is likely to eliminate any effective defense, counter attack, or human response; only an automated defense would work quickly enough to have any effect. (A Phillips, 2012).

In addition, with the rise of such asymmetric cyberwarfare in which different tactics are used, it is especially relevant for Australia to consider how to best use cyber means to effect deterrence within both peacetime competition and wartime crisis, given the country's delicate political and diplomatic dance with China. As Lupovici (2011) stated, cyberwarfare 'allows weak players to move the confrontation into a sphere in which they can maximize profits while risking little' (p. 52), which potentially makes cyber deterrence challenging to institute. Likewise:

> while China is a major economic partner for Australia, particularly with respect to trade, Australia aims to maintain a stable relationship with China even as it pushes back against Chinese influence and interference. But there is also growing concern in Australia that China's rising power and influence undercuts Australia's influence in the Indo-Pacific (Chase & Moroney, 2020 p. ix).

The absence of physical devastation or loss of life, the attacks occurring at light speed, the necessity for automated defences in the face of attacks that incapacitate effective defences means that strategy and process take priority placing. The literature is beginning to show the necessity for Australia to have strategic processes for deterring China in the cyber domain to offset the nature of the domain itself and the nature of cyber attacks.

Organising or structuring an approach for Australia in deterring China should involve careful strategic level planning that guides operational and technical levels. Therefore, investigating various frameworks is crucial to adding deeper understanding to the case studies of China and Australia that will come later on, before finishing with a discussion on the applicability of deterrence by punishment mechanisms. It is necessary to investigate various frameworks and assess the use value to the research questions posed in Chapter 1.

1.6 Deterrence Strategy and the Cyber World

As aforementioned, deterrence strategy emerged into the forefront during the Cold War; it was particularly prevalent among nuclear powers and prioritised the promise of retaliation, culminating in concepts such as mutually assured destruction (MAD; Van de Velde, 2023, p. 43). The concept of deterring an opponent either through the promise of retribution or through the denial of success through attacks has proved to be advantageous regardless of the domain of warfare. However, throughout the Cold War the focus was on nuclear deterrence and on

weapons that have exceptionally clear kinetic repercussions (e.g. MAD), which are ultimately not very nuanced vehicles of destruction.

Nuclear deterrence is distinctive to other methods of deterrence due to the chance that all actors will potentially die. Other methods of deterrence may not be as effective as they cannot guarantee the destruction of an antagonist. Therefore, the antagonist may ignore the deterrence in place or suffer the blow of the deployed deterrent mechanism, as the antagonist is not wholly destroyed and thus can suffer the malfeasance. The antagonist may also simply not understand the deterrent threat in the first place, owing to 'cultural barriers to understanding, internal preoccupations, or psychological distress' (Wirtz, 1993). Conversely, nuclear deterrence offers no such recourse.

In fact, nuclear deterrence can ignore the core components of deterrence theory, especially those regarding communication. Nuclear weapons are themselves the communicative element, and hence, there is no need to discuss aspects such as an actor's capabilities, deterrent mechanisms and nuance because the nuclear weapon offers such massively destructive potential that has been demonstrated (e.g. in Nagasaki, Hiroshima and further testing) that all actors understand the ramifications of using it (Stone, 2012, p. 116).

Libicki (2009) depicted a core issue to be observed in cybersecurity endeavours as follows:

> The ambiguities of cyber-deterrence contrast starkly with the clarities of nuclear deterrence. In the Cold War nuclear realm, attribution of attack was not a problem; the prospect of battle damage was clear; the 1,000th bomb could be as powerful as the first; counterforce was possible; there were no third parties to worry about; private firms were not expected to defend themselves; any hostile nuclear use crossed an acknowledged threshold; no higher levels of war existed; and both sides always had a lot to lose. (p. xvi)

Subsequently, Morgan (2003) cited six distinctive elements of nuclear deterrence:

1. Severe military conflict
2. Classical presumption of rationality
3. Guaranteed retaliation upon attribution
4. Concept of unacceptable damage
5. Credibility of responses
6. Stability of nuclear responses

All six elements are useful in breaking down the process of a nuclear retaliation. Of note for cyber-deterrence considerations is the presumption of severe military conflict and the concept of unacceptable damage. Currently, it is unclear and unlikely that a nation has cyberwarfare capabilities to inflict unacceptable damage, and there is no reason for severe military conflict to instigate cyber hostilities. Nuclear deterrence and MAD are not directly applicable to cyberwarfare but do appear to offer some degree of usefulness in a deterrence assessment which is that under the right conditions actors can assume some level of rationality or face total destruction (or perhaps incapacitation, as mentioned in the prior section).

By comparison, the cyber domain has numerous inherent difficulties. In particular, levels of attack can differ significantly and the state itself is not the only deliverer of cyber weaponry, as the private sector or non-state actors can potentially develop and deploy their own cyber weapons, such as the now infamous Pegasus software (Bergman & Mazetti, 2023). Concurrently, individual actors may work alone, which further complicates the threat surface. Thus, the cyber domain is a melange of public- and private-sector mechanisms and personnel. Indeed, for some, in the strategic considerations about how to deter, there is still significant debate over whether cyber deterrence is a functional concept or even a practical goal (Sheldon, 2012). Most states still tend to fall on deterrence-by-punishment measures that do not fit within the cyber domain, preferring to enact a more holistic approach to deterring potential antagonists (Flatgard B & Thomas-Noone, B, 2017).

Deterrence can be neatly summed up as a ‘relational variable’ (Gray, 2000, p. 255). Deterrence is the result of a particular relationship and has a shifting value. This relationship is often characterised as antagonistic and between various states, but in other circumstances it can also be applied in non-state arenas. Then, the shifting value of deterrence often refers to the ever-changing nature of power relations between states. For instance, as states develop weapons, it will affect their strategic considerations and the deterrence-based matrix—not only of the state’s own capabilities but also the capabilities and defences of other states—becomes more complicated. Furthermore, it is not just the completion of a specific innovation or development that affects strategic considerations—the ongoing development of new, modified and superior technological capabilities may also affect strategic outlooks and policy decisions.

For instance, deterrence theory in the post-WWII era is neatly summed up as a series of waves. The first wave of deterrence was the response to the development and deployment of the atomic bomb, which ushered in a new era of warfare and concepts of deterrence (Jervis, 1979). The

second wave emerged in the late 1950s to 1960s, in which concepts such as game theory were applied to develop what became conventional wisdom, at least in the West (Jervis, 1979). Game theory models aim to prescribe

> what a decision maker ought to do in a given situation, not what a decision maker actually does. To maintain nuclear strategic stability, it is of paramount importance to understand the dynamical interplay between all players involved in decision making processes with regard to nuclear strategy. (Lindelauf, 2021, p. 421)

In the third wave of deterrence, case studies were used to empirically test deterrence theory, mainly against cases of conventional deterrence and step-by-step iterations. This wave was particularly notable as it challenged many of the assumptions of the second wave, such as rational actor theory; rationality requires actors to be able to identify their preferences and judge for themselves the paramount ways and means to achieve goals (Knopf, 2010, p. 1). Thus, it is crucial to understand that deterrence strategy is not only incumbent on the capability of the deterrer but also that of the deterred. Gray (2000) followed this reasoning by asserting that 'the opponent is at liberty to make decisions that to us appear unreasonable' (p. 257).

Thus, Gray contradicted the views of the rational actor model, which asserts that actors follow 'known, familiar perceptions, norms, goals, and values, i.e., those that were deemed rational by Western observers' (K B Payne, 2011, p. 394). It has been argued that a fundamental flaw of deterrence strategy is that it relies upon the opposing actor being 'rational', which is a consideration for the deterrer that is heavily influenced by the prior actions of the antagonist and the assumption that the antagonist will follow the path of optimal rationality. Further, deterrence strategy relies on the assumption that an actor is deterrable, which is particularly problematic in the realm of conventional deterrence (Rhodes, 2000, p. 221). Moreover, when less deterrable actors acquire advanced cyber capabilities, they will likely intensify and increase their cyber attacks (Lewis, 2011).

The nature of conventional deterrence is that it regularly fails, even in cases where states have committed to a clearly defined deterrence policy that is openly publicised and have also stated their intention to defend by force (Lebow, 1985). Ultimately, there are overriding principles of deterrence. In short, deterrence is reliant upon the type of threat, weaponry or capacity and political willpower (Stone, 2012, p. 110).

Because of these variable components, deterrence has arguably three fundamental in-built premises:

1. Technical capability: Do we have the ability to carry out and deploy a deterrence mechanism?
2. Willpower: Is there sufficient political will to deploy our deterrence mechanism(s), and are our threats credible? (also see Stone, 2012, p. 109)
3. Communication: Is the antagonist aware of our deterrence mechanisms and our willpower to deploy them in certain scenarios?

This sort of framework encapsulates much of the deterrence debate. Deterrence mechanisms themselves have many different shapes and forms. Cyber deterrence may be the next such policy mechanism in contrast to conventional methods. Significantly, deterrence strategies will be affected by the specific actors and alliances involved: Australia may rely on the US to provide a nuclear umbrella that creates extended deterrence – future Australian strategies may benefit from considering the 'cyber umbrella' too (Hawkins & Kimber, 2016). Deterrence can also be in the form of punishment for actions or in the form of denial of actions (Rhodes, 2000). Unpacking two particular systems of deterrence—namely, punishment and denial—relative to the cyber domain will have significant ramifications for Australian strategy.

In summary, the organisational and technical realities of cyberspace have transformed considerably. In efforts to delineate the deterrence mechanisms within cyberspace, deterrence by punishment is the concept 'that one party deters another from acting by threatening to damage the other party to such an extent that the positives of any antagonistic outcome are outweighed by the retribution' (Morgan, 2003, p. 1). Further, deterrence by denial is the concept 'of making an attack so difficult that the prospective gains to be made are outweighed by the costs of launching an attack' (Stevens, 2012, p. 150).

Further, in diverging from more conventional theoretical approaches, an interrelated and recurring issue in cyberspace is attribution, which can make deterrence by punishment more challenging or difficult to enact (Libicki, 2009, p. 7). Therefore, some consider deterrence by denial a more 'desired' form of deterrence although deterrence by punishment and deterrence by denial can and often do work in concert with one another (Libicki, 2009, p. 8).

Ultimately, it can be argued that as state actors try to use cyber attacks to achieve advantages over one another, an effective and integrated deterrence strategy will incorporate both aspects

of the theory. In practical terms, there is little sense in going on an all-out offensive and believing that to be the best defence, nor is all out denial alone likely to be enough as a deterrent mechanism. Regardless, it is important to remember that deterrence strategy in any shape or form is primarily about trying to shape the behaviour of an adversary (Lebow, 2005, pp. 765–766). As Mandel (2017) added, a cyberthreat does not exist in a vacuum, and hence, responses should be formulated and implemented in the context of larger global security affairs—in this case, such a security setting is explicitly connected to the Australia–China relationship.

1.7 Deterrence by Punishment Frameworks with Cyber Purposes

Deterrence in cyberspace must consistently address recurring themes across various scholars:

Joseph Nye states cyber deterrence depends on perception, attribution, uncertainty, and escalation risks and should consider entanglement and norms (2016). Will Goodman contends that real-world examples demonstrate cyber deterrence is viable, but challenges include attribution, anonymity, scalability, reassurance, escalation, and clear signalling (2010). Conversely, Michael Fischerkeller and Richard Harknett argue that the uniqueness of cyberspace makes deterrence unfeasible below the use-of-force threshold, theorizing that continuous interactions encourage stable competition (2017). Mariarosaria Taddeo reasons deterrence is limited by the nature of cyberspace regarding attribution, credible signaling, escalation, uncertainty of effects, and proportionality (2018).

Systematising an approach to deterrence in the cyber domain is an important step for Australian strategy. The capacity to consistently deter potential threat actors like China will be further established throughout the thesis, as well as the requirement, but as discussed earlier the functional usefulness of cyber-deterrence is often in question. Differing frameworks have offered different justifications and are useful for determining the proposed use value of deterrence by punishment in the cyber domain however, there is still robust debate in scholarship about the concept of deterrence in cyberspace, and the seeming lack of feasible practical solutions (Soesanto & Smeets, 2020, p. 385).

The aforementioned text from Soesanto & Smeets is a short exploration of cyberdeterrence and begins its penultimate section with the assertion that the writing and thinking about cyberdeterrence is slowly falling out of fashion among scholars, and that this trend is likely to

continue (2020, p. 394). Importantly, the authors argued that cyberdeterrence discourse is likely to track in four distinct pathways:

1. Incorporating cyberdeterrence as an element within broader international security,
2. Deterrence efforts that can be primarily achieved on the operational and technical level,
3. Shifting away from deterrence towards compellence,
4. Strategic concepts that seek to contain and blunt adversarial aggression in cyberspace that stands apart from traditional deterrence thinking (ibid, 2020, pp. 394-395).

Strategic cyberdeterrence is of particular interest in an investigation on the feasibility of the concept applied to a case-study between nation states like this thesis intends to do. Without disregarding the useful and potentially insightful avenues of investigation that all four above pathways proffer, this thesis has from the outset intended to remain at the strategic level and is informed by the operational and technical levels. The case study of course is situated within broader international security, but remains in the cyber domain. Finally, the thesis is investigating deterrence and not other concepts like compellence.

With this in mind, Libicki's framework functions as a useful tool for achieving the objectives of the above paragraph.

Cyber-deterrence and cyberwar are consistently discussed topics however, systematised approaches to deterrence by punishment are at time of writing not. The development of deterrence literature is still underwhelming despite sporadic bursts of interest, and part of this is blamed on deterrence scholars struggling to argue if cyberdeterrence theory is based on evidence collected from the cyber domain rather than deduced from known outcomes (Soesanto & Smeets, 2020 p. 397). The field is still relatively young to even other waves of deterrence post-WWII, let alone deterrence as a study itself, and investigating strategic level systems that can assist countries like Australia bear relevance. The literature is lacking in a case-study analysis of these strategic level systems and then answering the feasibility of cyberdeterrence.

1.8 Conventional Deterrence

Conventional deterrence refers to deterrence by military superiority. By default, it is much less likely than nuclear deterrence to result in a stalemate; instead, conventional deterrence produces a 'fluid' strategic interaction. Consequently, it fits closely to the overall model of deterrence as a relational variable (see Harold, Libicki, & Cevallos, 2016).

In conventional deterrence, examples are required in order to further communicate threats, and these examples must also then be analysed against the antagonist's capabilities (see Harknett, 1994, pp. 88–89). This assessment against the antagonist's capabilities emerges from the antagonist themselves—for the deterrer, much of the threat comes with the assumption of knowledge about the antagonist's capabilities. Ultimately, however, the deterrer reveals more information than the antagonist about capability, potentially granting the antagonist an information advantage (assuming that the deterrer does not already have in-depth knowledge of all parties via espionage or other means; see Rhodes, 2000, p. 227). Hence, conventional deterrence has a high informational burden (Shimshoni, 1988, p. 16). This is potentially troubling for the cyber domain, as revealing knowledge of capabilities, even of systems the deterrer could target, may nullify the deterrent mechanism (Libicki, 2009, pp. 52–53). Therefore, it would appear that conventional deterrence offers a modest and limited contribution to deterrence models, particularly as more actors are implicated in the deterrence model and more informational difficulties might rise (Stone, 2012, p. 109).

In particular, troublingly for conventional deterrence, state actors interested in changing the status quo (e.g. China) normally have more than one option for doing so:

> The relevance of this observation to the design of defenders' deterrence policies is self-evident. The defender's strategy must be made relevant to the range of alternative options possibly available to the initiator. A deterrence policy which discourages an opponent from employing some options but not others is incomplete and may not prevent a failure of deterrence. (George & Smoke, 1974, pp. 520–521).

Therefore, conventional deterrence is reliant on a holistic approach to deterrence in which the deterrer utilises much of their resources in order to deter the antagonist. Thus, measures taken to deter one option may be detrimental to deterring others. Furthermore, conventional deterrence is heavily reliant on explicit 'red lines'—that is, markers that indicate the tolerance levels of states for aggression (Harknett, 1996). In liberal democracies such as Australia, the

‘tolerance’ level of a state is not only incumbent on the executive and its military but also affected by the electorate, who can create public opinion and contribute to these red lines. Hence, antagonists can exploit these political effects, keeping the antagonistic actions outside the threshold for retaliation (see Rhodes, 2000, p. 232).

Rhodes (2000) also asserted that a structural feature of the strategic interaction of deterrence is that the deterrer must reveal information about capabilities and strategies, whereas the antagonist does not. In particular, this is a strategic interaction ‘in which capabilities are constantly evolving, in which potential aggressors are free to develop multiple options, and in which deterrers must address multiple audiences’ (Rhodes, 2000 p. 233). The result of this feature is that the rules of the strategic competition are skewed in the antagonist’s favour—all the antagonist requires is to perceive a workable option, and then, the deterrent mechanism fails to deter.

It is especially problematic when multiple actors are involved, as the presence of more actors has a multiplicative rather than an additive effect in deterrence, drastically increasing the difficulty for the deterrer. This, in turn, has three critical ramifications for deterrers who are attempting to make deterrence work:

1. The antagonist ignores the deterrers interests and is only invested in pursuing their own strategic goals regardless of any deterrent mechanisms that may be in place.
2. The antagonist ignores the historical record of the deterrer regarding the deployment of deterrent mechanisms and following through on threats.
3. The antagonist entirely ignores the capabilities of the deterrer, ignoring not only the deterrer’s will but also their technical prowess. This ramification links to the antagonist’s analysis that despite it being a smaller power, the gap between powers is widening to such an extent that it behoves the antagonist to launch an attack, for attempting to ameliorate the growing capability gap (see Rhodes, 2000, pp. 236–237).

Last, deterrence may be analysed as ‘successful’ in allowing a degree of uncertainty on the part of a would-be aggressor, when escalation is avoided and when used in coordination with other foreign policy tools. Conventional deterrence theory can be utilised in the assessment that conventional deterrence is not a static process but rather, a dynamic one (Wirtz, 1993).

Ultimately however, conventional deterrence appears as a fragile condition, wherein an actor may successfully deter an antagonist until the latter assesses that the current simulacrum can

no longer continue on a cost–benefit calculus. Hence, the antagonist may then begin launching attacks anyway, and the deterrent mechanism will fail. The antagonist may be pushed to action owing to their assessment that if they do not act, they might even fall behind in terms of capacity, or owing to their assessment that they can absorb the deterrent mechanisms. Furthermore, the antagonist may be incapable of assessing the deterrent threat because of cultural, ideological or informational deficiencies that block their ability to be deterred (Knopf, 2013). These issues result in conventional deterrence offering an ultimately tepid contribution to a state's defence and security strategy.

1.9 Extended Deterrence

Australia has long considered the concept of extended deterrence adding to the strategic considerations of potential adversary nations. In particular, the ANZUS alliance in 1951 clearly stated that the US, Australia and New Zealand would 'consult' about one another's defence.

Throughout much of the 20th century, extended deterrence was implicitly tied to conventional invasion and attack, and much of Australia's considerations of this strategy was in relation to Japan and Indonesia (Frühling, 2013, p. 18). As Huth (1988) asserted, an extended deterrence confrontation 'entails an overt threat and counter-threat by potential attacker and defender'. The US provided this extended deterrence to Australia and other allies in Asia and elsewhere. Indeed, the US provided assurances of extended nuclear deterrence to its major allies from the beginning of the Cold War (Beazley, 2003, p. 329).

While the effectiveness of extended deterrence is still unclear—for instance, it is uncertain when a cyber attack may result in an armed attack—Australia has appeared very willing to engage with the idea of a security 'guarantee' and related deterrence value. Even if it is considered that a cyber attack on Australia, the US or New Zealand would trigger the ANZUS mechanisms and that these countries would consider a mutual response to a cyber attack (see Rudd & Smith, 2011), the threshold for an armed response to a cyber attack is not lucid or publicly discussed.

Nonetheless, Australia cannot, and does not, act in isolation in dealing with cyberthreats. Citing the recognition of the cyber domain as of critical importance to defence, economic and societal considerations, the 2011 statement declared that 'in the event of a cyber-attack that threatens the territorial integrity, political independence or security of either of our nations', the two

allies would work mutually to determine ‘appropriate’ and presumably proportionate responses (Rudd & Smith, 2011). Political independence is a particularly interesting point—in 2016 when it was alleged that Russia had interfered in the US election through cyber means, ANZUS was not invoked, and the US retaliation response to election interference has proved an incredibly difficult issue (see Sanger, 2014).

Overall, as the focus of the Australia–US alliance turns to the challenges associated with China and the Indo-Pacific, most Australians do see ANZUS as a vital and dependable foundation of Australia’s security—even if it is ambiguous (Jackman, 2021). In applying the ANZUS,

> lumping everything under the single heading of ‘cybersecurity’ makes the domain simultaneously seem more homogeneous than it actually is and intractably large. Ideas that are in practice quite disparate are conflated and, as a result, policy prescriptions are too general to be useful. In this environment, it’s not surprising that the joint statement is a little vague. But when cyber-attacks are elevated to the level of ANZUS, it’s especially important to understand precisely what’s meant. (Davies et al., 2012, p. 4)

1.10 Cyber Deterrence, Risk Management and Cybersecurity

Cyber deterrence as a concept is comprehended broadly. Sharing this view, Dunn (2005) stated that ‘there is no generally accepted definition of cybersecurity, and several different terms are in use that have related meanings, such as information assurance, information or data security, critical information infrastructure protection’ (p. 2).

Nonetheless, the objective of Australia’s cyber-deterrence efforts is to prevent cyber activity that is damaging to its interests. A burgeoning cyberthreat matrix has led organisations such as the United Nations to invoke resolutions in order to ‘determine the cybersecurity and critical information infrastructure protection risks to your economy, national security, critical infrastructure and civil society that must be managed’ (United Nations General Assembly, 2010, p. 3). However, in this context, cybersecurity risks can be managed or minimised but cannot be eradicated, and cyber deterrence can carry a risk of unintended escalation.

In creating an effective strategy, a computer network also cannot be protected by a single security measure. While the purpose of risk assessment is to then help to inform relevant stakeholders, according to Ross (2012), risk management is a comprehensive process requiring organisations, including defence, to

1. frame risk (i.e., establish the context for risk-based decisions);
2. assess risk;
3. respond to risk once determined; and
4. monitor risk on an ongoing basis using effective organisational communications and a feedback loop for continuous improvement in the risk-related activities of organisations (pp. 4–5).

Thus, the purpose of risk management is 'not to eliminate all risk. It is a tool to be used by management to reduce risk to an acceptable level' (Peltier, 2005, p. 5). In other words, cyber attacks may occur even in presence of sophisticated deterrence measures. Thus, 'success' is about the impact on adversary behaviour, imposing costs and risk mitigation rather than complete elimination, which involves affecting the adversaries' strategic decision-making, imposing greater amounts of risk and designating thresholds for potential adversaries to not perform actions that they may want to, but which the deterrer does not want them to perform.

In addition, while multiple definitions of cybersecurity may not be an obvious drawback, the absence of a concise, standard definition may 'impede technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges' (Craigen, Diakun-Thibault, & Purse, 2014, p. 13). Hence, at the very least, accurate risk assessment will be vital for strategic decision-making because erroneous and 'unreliable information resulting from wrong security policies generates uncertainty and mistrust, and has a negative impact on every business area' (Mellado & Rosado, 2012, p. 1599).

Consequently, despite a global response to cybersecurity threats, there is still a significant gap in the knowledge of decision-makers about not only the ramifications of migration and deterrence strategies employed but also the effectiveness of these strategies and the role of risk management. Associated difficulties such as a lack of shared norms in cyberspace (and the inherent difficulty of attribution methods) also make individual or coordinated efforts to police and manage the domain increasingly challenging. Establishing norms will be a component of successful deterrence by denoting mutually accepted practices accepted and conducted by states (Van de Velde, 2023).

This is despite much of the international community, including the five permanent members of the United Nations Security Council, and the United Nations General Assembly, having agreed

on a framework for responsible state behaviour in cyberspace. It is worth noting that Australia's 2017 International Cyber Engagement Strategy did express a commitment to diplomatic action 'to support an international cooperative architecture that promotes stability, and responds to unacceptable behaviour in cyberspace. In responding to malicious cyber activity, Australia will seek to engendered greater compliance with the rules and norms agreed at the UN' (Department of Foreign Affairs and Trade [DFAT], 2017b, p. 2, Annex B). This position notes that when responding to a use of force:

> Australia considers that the thresholds and limitations governing the exercise of self-defence under Article 51 of the UN Charter apply in respect of cyber-operations that constitute an armed attack and in respect of acts of self-defence that are carried out by cyber means (Department of Foreign Affairs and Trade, 2017b, p. 3, Annex B).

Accordingly, cyberspace should not be akin to the Wild West. China is also increasingly underscoring the importance of government sovereignty in regard to cyberspace and data (Zaagman, 2020). Cyber can be an instrument for war. If cyberwarfare is

> limited to enabler status, other operational intent will drive the execution towards the strategic goal. Cyber capabilities offer a strategic opportunity that will grow in coming decades. Cyber effects will be limited if subordinated to enabler status and by doing so provide democracies reduced military options. (Kallberg, 2016, p. 113)

Simultaneously, cybersecurity, cyber espionage and cyberwarfare all remain ongoing areas of conflict and competition and are among the most diffuse, difficult areas to establish a stable and secure consensus relationship between different powers (Austin, 2023; P K Davis, 2015, p. 334; Galloway, 2021). Furthermore, signalling can be misperceived. Despite the fact that policymakers worldwide have toughened risk management measures in the cyber realm, 'predicting the future is hardly possible, but stating that cyber aggression – be it espionage, sabotage or even warfare – will be a continuing threat to international security and stability in the coming years seems a safe forecast' (van der Meer, 2016, p. 95).

In the Australian setting, cybersecurity has been labelled as protection from 'cyber attack', defined by the ACSC (2016) as 'a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity'. Austin (2016) also posited that cyberwarfare itself is 'the continuation of politics through cyber means

with warlike intent. Cyber means must involve "machine-based computation" with or without support from kinetic military capabilities' (p. 26). However, Austin (2016) asserted that cyberwarfare that is independent of non-cyber domains is 'unimaginable'. This distinction that Austin posited can lead to a problematic view about cybersecurity among many Australian decision-makers:

> One senior defense official said that active defense is akin to being in a battle zone when someone is firing a machine gun at you, detecting the bullets, putting up a shield and knocking down the bullets. 'Wouldn't it be a far better idea to get the machine gun? So that's an extension of a real-time defense – just shut the threat down'. (Nakashima, 2010)

The comparison between kinetic and cyber operations is awkward, since cybersecurity does not adhere to the same rules and conditions of kinetic operations, which has ramifications for risk management and deterrence attempts.

Cybersecurity is potentially complicated by the fact that much of military doctrine and prevailing attitudes have been heavily influenced in, and informed by, the kinetic domains of warfare, and again, risk assessment is still a contested area of discussion in the geo-strategic space (Hayden, 2011). Yet, as explored later in Chapter 3, China desires a greater capability and autonomy in the cyber domain, as 'the nation aspires to obtain the best technologies in the world' (Zuo, 2016). Interestingly, some military actors such as former US Lt. Gen. Wyche have posited:

> We are entering a new era of evolving threats, advancing technologies, and reduced resources. Adversaries continue to exploit weaknesses within interconnected systems, such as the Enterprise Resource Planning solutions that now power the Army's daily operations through the aggregation and analysis of vast amounts of data, sometimes from frozen sources. Each of these sources brings its own level of threat and vulnerability, leading to an incredibly complex environment ripe for exploitation. (Wyche & Goss, 2016, p. 15)

Therefore, as computer and technology systems becoming progressively complex and interconnected, opposing state actors' capacity to exploit these systems and uncover critical information will increase. Significantly, Wyche and Goss (2016) asserted that 'we must take aggressive steps to better protect our essential data' (p. 15), which will also add risk intricacy and escalation dangers to the system and further complicate the situation. Further Rid (2012) offered an insightful finding that the 'higher the technical development and the dependency of

a society and its government and military, the higher is the potential for sabotage, especially cyber-enabled sabotage' (pp. 14–15).

This finding is perhaps exemplified in Rid's (2012) own analysis of the Russian invasion of Georgia in 2008 and the concurrent cyber attacks on Georgia—owing to the relatively underdeveloped nature of Georgia's cyber infrastructure, there was very little significant damage and disruption that the cyber attacks could actually achieve. Rid summarised that cyber conflicts are not in fact an 'act of war', but can instead be divided into three distinct categories, espionage, subversion and sabotage, none of which fits within the traditional definition of warfare (p. 5). This definition stipulates that to be considered an act of war, an attack must be violent in nature, be instrumental in that there is a means to an end (wherein physical threat or violence is the means) and that the action must be political in nature (Rid, 2012, p. 7).

The only above three-tiered avenue that cyber attacks could possibly satisfy is the political element. Nevertheless, as Rid (2012) stated, even this element is frequently missing as cyber attacks are often clandestine in nature and attribution can be vague or fail to identify who the precise attacker actually is, thereby nullifying the 'political' effect of the attack. This is also significant to deterrence theory, as one of the noted difficulties for implementing deterrence strategy relates to the ability to communicate capabilities to possible aggressors and deter them from engaging in aggressive acts; in fact, it is possible to even argue that threatening punishment contributes to international instability (see Nevill & Hawkins, 2016, p. 5).

In contrast, Sharma (2016) asserted that cyber capabilities can operate within the definition of conventional warfare, in that cyber operations can still achieve the overall objective of utilising power to compel an enemy to act as the opposing nation wills (p. 57). For instance, for the military component, the heavy reliance on IT systems to carry out operations and coordinate the movement of troops is an exploitable and vulnerable arena. Sharma stated that cyberwarfare can be effective in deterring, denying and disrupting key functions to an opposing country, which could lead to a '*cascade effect* [emphasis in original], resulting in chaos, anarchy and bedlam in the victim nation … will generate the desired end result of compelling the enemy to submit to your will' (pp. 65–66).

Overall, the concepts of cyberwarfare and cybersecurity are inconclusive and fluid. Yet, as Wildi (2023) noted, 'cyber operations have become an indispensable element of modern conflict' (p. 124). However, these operations have weaknesses, given that cyber weapons

typically have a ‘once-only’ factor applied to them; that is, the weapon is useful only as long as the vulnerability in the target system exists, which limits the repeat usage of weapons and also heightens the strategic ramifications in the use of highly sophisticated cyber attacks (Seligman, 2022). Nonetheless, from a strict ADF perspective, an effective cyber-deterrence framework would aim to safeguard Australia’s capabilities to fight wars and ensure that such critical infrastructure would perform and survive against malicious actions in cyberspace.

1.11 Moving Forward

Therefore, can Libicki’s cyber-deterrence framework assist Australia in discouraging China from engaging in strategic-level cyber attacks and cyberwarfare operations? The following chapters will be devoted to providing this context and analysis and establishing where each actor stands in terms of relative capacity, power and leverage in the cyber domain, before establishing what is known as attribution and related challenges in cyberspace. China’s and Australia’s development of cybersecurity practices, policies and technologies will be investigated, as will the credibility and applicability of attribution tactics, techniques and procedures, in order to inform the deterrence framework analysis in Chapter 5. Cyber deterrence is challenging, and there are stark differences between it and nuclear deterrence, but for Australia, an achievable and necessary endeavour is to create a legitimate, credible capability to impose costs on adversary nations such as China.

Chapter 2: Cybersecurity Policy Developments in Australia

2.1 Introduction

The cyberthreat landscape has shifted and changed dramatically, and for Australian policymakers, it has evolved from cybersecurity concerns over domestic hackers and transnational criminal enterprises to multi-factor state-based offensive cyber operations by countries such as China and Russia. To rise to this challenge, Australia has engaged in many major policy developments to increase its capacity to defend against cyber attacks, facilitate better cyber resilience and enhance its ability to deter malicious cyber operations. These developments cover the spectrum of people, processes and technologies to act as a comprehensive cyber-deterrence capability.

This chapter will address the evolution of such policy developments, focusing on official cybersecurity guidelines and consecutive white papers related to cyberthreats, cyber governance, 'thresholds', offensive measures and the development of interrelated IT and communications technologies.The examination of such policy and legislative responses will primarily begin from the 2000 DWP, which is the first significant 'official recognition' of cybersecurity as an important national security issue, and will include policies in 2023, with the aim of exposing the design of the Australian Government's pursuit of cybersecurity.

The chapter's ambit will also sit within the scope provided by the Libicki (2009) framework, which as stated in Section 1.1, defined the assessment for strategic cyberwar that can affect the target state's behaviour (Australia) and the capacity for the target state to deter other states (China) from engaging in cyber attacks against it and the exploitation of its vulnerabilities (see Libicki, 2009, p. 5). As Nevill and Hawkins (2016) stated:

> The use of deterrence to mitigate security threats is based on an assumption that states are rational, and make decisions based on cost-benefit assessments. On that assumption, one can deter a challenger by increasing the perceived costs of their action (deterrence by punishment) or decreasing the expected benefit (deterrence by denial).

Thus, the evolution of Australian cybersecurity strategy/policy—what the Australian Government has done and is doing in cybersecurity to create disincentives for China—which is illustrated via key strategic objectives and guiding policy principles, remains crucial to understanding deterrence-by-punishment and deterrence-by-denial mechanisms, in particular,

and identifying existing communicated intent/capabilities (and those that might be required for future deterrence considerations). Hence, this chapter will investigate how Australia has incrementally developed its cybersecurity and cyberwarfare objectives, priorities and capabilities in a threat landscape in which the country has aimed to align such developments with the possible actions that it can take, in part, to avoid crisis escalation and to deter China more effectively from engaging in what Libicki (2009, p. 117) described as strategic cyberwar.

In this regard, official policy documents such as the Australian Government's Cyber Security Strategy 2020 do provide a historical roadmap of the government's mindset regarding, and design of, threat assessments (Department of Home Affairs, 2020). For example, the 2020 Strategy (2020) did build on the 2016 Strategy that comprised enhanced cybersecurity obligations for entities considered to be involved with critical infrastructure of national significance (Department of Home Affairs, pp. 7-8). Further, these documents reveal some insights into the credibility of cybersecurity and corresponding objectives in order to prevent, respond to and deter cyber activity (and thus to help shape international behaviour, including that of actors such as China). Furthermore, by analysing key documents aiming to identify cyberthreats and build cybersecurity capabilities, the investigation in this thesis will cover some of the public reactions and communications surrounding policy efforts to establish deterrence postures and stability in cyberspace.

In broad terms, Australian security goals since 2000 concerning cyber intrusions can be seen as defending networks, building resilience and then fostering the advancement of defensive (and noted below later, offensive) cyber-attack capabilities, which will add to a level of deterrence that was initially aimed at disrupting and deterring organised offshore cybercriminals (see Turnbull, 2017) and then morphed into dealing with state-based threats, such as those from China, under former Prime Minister Morrison and his Cabinet (M Payne, Andrews, & Dutton, 2021).

It also worth repeating that Australia's offensive cyber capability resides within the ASD and Project REDSPICE (Australian Signals Directorate, 2023). Nevertheless, as a starting point in addressing threat information and deterrence strategy, the internet at its creation was intended to be a means for rapid communications and the consistent transfer of public information, and thus, secure communications and protected information networks were not a core priority at first (see M Thompson, 2012). In the 21st century, with critical infrastructure becoming intrinsically linked to the cyber domain, the capacity for malicious attacks from state (and non-

state actors) has been on an ever-increasing trajectory, with the current Albanese Labor Government announcing that cybersecurity is today a 'whole-of-nation' endeavour (Hendry, 2022; Libicki, 2009, p. xiii).

In general terms, Australia's broad perspective on international cyber engagement has been to promote an open, free and secure cyberspace (Department of Foreign Affairs and Trade, 2017b, p. 7). Thus, many white papers and strategic documents have recognised that Australia's increasing dependence on information systems is creating both new opportunities as well as adaptive threats and extended vulnerabilities. For example, in capturing an 'active defence' mindset, the 2016 Cyber Security Strategy highlighted that that Australia's 'defensive and offensive cyber capabilities enable us to deter and respond to the threat of cyber-attack' (Department of the Prime Minister and Cabinet, 2016, p. 28).

2.2 Key Policy Challenges

For cyberwar to assume strategic importance, it must be able to generate affects that are at least comparable with, and preferably more impressive than, the effects generated through kinetic means. Showcasing capabilities in cyberspace will also be vital, and the Australian prowess to detect, defend against and respond to hostile acts must be well known or there can be no deterrence (Van de Velde, 2023). Decision-makers must also be aware about ways to request the deployment of cyber means, the extent to which the deployment can be controlled (i.e. whether it will have cascading effects or can be restricted to one environment) and whether they can clearly communicate the nation's ability to conduct these operations with enough opaqueness such that the capabilities of the cyber weapon are not immediately nullified (Seligman, 2022).

Overall, systems and networks are highly connected currently. Much of modern-day government policy is repeatedly pitched as being committed to defending critical infrastructure in Australia, which includes the central systems that support the economy and that most Australians still rely on in their day-to-day life, including the digitisation of social and related communications networks and the connectivity of banking, finance and related utilities (see Department of Home Affairs, 2020, pp. 5, 6, 13). Therefore, the destruction, degradation or denial of access to the cyber landscape of these facilities, supply chains and IT and communications networks will adversely affect Australia's interests. Capacity and communication are key challenges in resorting to a cyberwar, given the increased dependency

on computer systems, the scale and rate of new vulnerabilities and the ability for malicious actors to potentially evade attribution, which refers to the process of tracking and identifying perpetrators of a cyber attack (see Alazab, 2022).

Thus, Australian policymakers face a conundrum: How can Australia promote a free, secure cyberspace as well as norms of 'good behaviour' on the international stage while concurrently defending the cyber components of its critical digital infrastructure from cyber-capable enemies and addressing related deterrence challenges? Efforts to identify intrusions and threats will incorporate how existing rules, principles and norms of behaviour in the political realm could or might be extended into the architecture and administration of the asymmetric cyber world and the protection of 'non-combatants' in a nonviolent setting (Dinstein, 2012, p. 261).

As regards issues of communication and the deployment of autonomous weapons and security in cyberspace, it was noted that Australia 'has an increasing dependence on an increasingly vulnerable cyber domain' (Defence Science and Technology Organisation, 2014). Furthermore, in the 2020 Cyber Security Strategy, it was stated that 'cyber security is at the heart of the transition to a digital society' (2020) and that cyber operations raise many political and security (and ethical) dilemmas (Department of Home Affairs, p. 10).

Certainly, by digitising critical infrastructure, the scope and scale of the provision of essential services has drastically improved for many Australian citizens (Department of Home Affairs, 2020, p. 4). However, it has also created a modernistic threat environment and extended opportunities for significant cyber attacks, ranging from botnets (i.e. hijacked internet-connected devices) to ransomware and large-scale phishing campaigns. In addition, the danger of strategic cyberwar, which Libicki (2009) defined as affecting behaviour and the strategic assets controlled by states via state-on-state cyber attacks (p. xv), remains a persistent concern for Australia. This includes the construction of well-defined and meaningful costs to deter perpetrators, particularly actions that would satisfy as an effective deterrence-by-punishment framework to mitigate threats.

For instance, in the 2020 Cyber Security Strategy it was announced that Australia would re-evaluate the balance of power in the Indo-Pacific and that the ASD would 'recruit 500 additional intelligence and cyber security personnel at a cost of $469.7 million over 10 years' (Department of Home Affairs, 2020, p. 24). It would also invest AU$385.4 million in enabling and enhancing intelligence capabilities (Department of Home Affairs, 2020, p. 24). This policy

framework was aimed at supporting operational and contingency plans that could involve wartime counter-military cyber operations against a cyber-capable opponent as well as (proportionate) retaliation against this opponent for attacking Australian systems.

Therefore, beyond debate about capacity and resourcing, it is also essential to address the messaging, credibility and communication aspects of any official strategy. In other words, if adversary states are 'in the dark' and unaware of at least some capability in deterrence dynamics, then the possible political message or diplomatic manipulation sought through deterrence by punishment will be compromised or wasted. In short, conveying a credible signal to the 'right' opponent remains an essential module for deterrence (Libicki, 2009, pp. 75–77**).** Libicki (2009) also argued that state actors subject to a cyber attack should also initially attempt to relay to the aggressor that the damage was minimal or marginal.

Therefore, effective deterrence hinges to a strong degree on the defender reliably signalling its intention to use its capabilities against the aggressor as well as actions related to communicating the limited impact of the attack itself:

> The reliability of a state's commitment to enforcing its own deterrence policy statements is a significant symbol of its political and military power. If a state doesn't follow through on a threat when its threshold is crossed, it directly reduces its credibility in the eyes of the international community, undermining its ability to both intimidate and negotiate in the future. (Nevill & Hawkins, 2016)

In 2016, the Australian Government explicitly committed itself to promoting international cooperation in targeting cybercrime networks, advancing stability and peace in cyberspace (assumingly between states) and utilising a coordinated engagement with like-minded private partners such as the US to enhance cyber resilience across the full spectrum of cyber affairs (see ACSC, 2016). Given the borderless nature of cyberspace, the revisited coordinated policy approach indicated an 'all-of-government' methodology, whereas the 2017 International Cyber Engagement Strategy reflected the notion of cyber affairs as a strategic international policy subject (Department of Foreign Affairs and Trade, 2017b, p. 5). This 2017 approach also aimed to make a strong statement about how international law applied to cyberspace by adding that 'achieving that cooperation requires creative thinking to build a flexible range of existing and novel response tools, and a nimble coordination mechanism to implement them effectively' (see Feakin, 2017).

In its ambit related to international security and cyberspace, this 2017 strategy again highlighted the benefits of a stable, peaceful online environment by setting clear expectations of state behaviour in cyberspace with ideas about increased transparency as a useful way to build collective confidence that agreed norms regarding acceptable or unacceptable behaviour in cyberspace would be adhered to (Department of Foreign Affairs and Trade, 2017b, p. 6). Practical confidence-building measures were defined as actions that 'foster trust between states to prevent misunderstandings that could lead to conflict' (Department of Foreign Affairs and Trade, 2017b, p. 52). Further, DFAT (2017b) defined such unacceptable behaviours as that of state actors who 'pursue their objectives by undertaking malicious cyber activities contrary to international law and identified norms of responsible state behaviour' (p. 54).

Notably for China, this is best described as 'rob, replicate and replace'—that is, malicious cyber activities largely driven by the seizure of intellectual property and the use of state resources to give competitive advantage to Chinese corporations (Demers, & Evanina, 2020). Therefore, Australia signalled its capacity to collaborate and engage in a coordinated capacity response to address malicious actions in the cyber domain, as a confidence-building deterrence measure that China and others would need to consider in assessing the country's strike and response competence. Thus, any deterrence strategy must identify existing policies and frameworks that demonstrate such a 'best-practice' approach to multi-stakeholder governance and related international cyber and technology communication challenges.

Similarly, when deciding Australia's key international cyber and critical technology objectives, it should be noted that concurrent to alliances and defensive development is offensive development: cyberwarfare operations that are, and will be, useful as an additional component to kinetic warfare (Department of Defence, 2021). Given the overlapping policy objective of sharing cybersecurity information with international partners and the rise of offence persistency in cyberspace, policy attention to shared vulnerabilities and greater cooperative methods of cyber deterrence in keeping the virtual commons safe is essential to counter Chinese A2/AD (area access, area denial) capabilities, especially in the South China Sea (see Gombert & Libicki, 2014, p. 8).

When attempting to strengthen practices of deterrence, it should be also noted that Libicki (2009) highlighted the importance of aspects peculiar to computer versus computer cyberwar that can affect the strategic decision-making of states, such as in controlling the risk of escalation and the extent of the defender's reaction (p. 125). Others have also noted the

development of a ‘escalation ladder’ that would initially attempt to identify the attacker and their objective. For instance, ‘industrial espionage may not require a declaration of war, but sabotage of the power grid may require more than a denial-of-service attack’ (see Kostyuk 2018, p. 124).

Last, on examining the different policy roadmaps of cybersecurity since 2000, it appears that cyber-deterrence solutions have ben ad hoc and have not always been coherent or even transparent. In other words, while Australia’s involvement in deterrence and related security aspects has been relatively steady, it can also be argued that ‘successive Australian governments have been unable to come to terms with the full import of the digital revolution … even though our major ally, the United States, began a clear transition in the mid-1990s’ (Austin, 2016, p. 1). It can be reasonably inferred at least that thanks to Australia’s relationship with the US and Five Eyes, Australia’s capability has evolved and steadily fused although it has struggled to develop its cyber power particularly when measured against states such as China (Uren & Price, 2018). Nevertheless, the 2022 announcement of REDSPICE (explored in Section 2.8) does signal forward-looking and potentially highly advancing domestic capabilities.

2.3 White Paper in 2000 and Peripherals

The first noteworthy ‘official recognition’ of cybersecurity as a national security issue emerged in the 2000 DWP entitled *Defence 2000: Our Future Defence Force* (see Brangwin & Portillo-Castro, 2019). Certainly, the 2000 DWP was significant in its identification of information and cybersecurity as a core responsibility of the defence sector, essentially tying it to the US approach and determining the cyber realm as an extended domain of warfare—a domain for which then Prime Minister John Howard had directed cyber capabilities to be preserved, reviewed and upgraded (see Church, Brangwin, Dyer & Watt, 2015, p. 40).

The 2000 DWP opened with the assertion that the government ‘had become concerned that a mismatch had arisen between our strategic objectives, our defence capabilities and our levels of defence funding’ (Department of Defence, 2000, p. vii). It added that Australia has ‘a significant national advantage. Our workforce … are highly educated and skilled in the use of information technology’ (Department of Defence, 2000, p. 94). The 2000 DWP was also precise in emphasising ‘we have access to excellent software and integration skills. So this is an aspect of military capability in which we can and should aim to make a difference’

(Department of Defence, 2000, p. 94). Importantly, the 2000 DWP discussed not only human capacity and the military's capabilities but also the possible effects of attacks on the civilian populace, perhaps foreshadowing the cost–benefit calculations of deterrence and the government's understanding of the real-world effects of cybersecurity in the public–private space.

However, the word 'cyber' itself appeared only three times in this DWP, and even then, in still some very vague open-ended assertions such as 'defence will be among the key contributors to the Government's efforts to develop responses to cyber-attack on Australia's critical information infrastructure'. (Department of Defence, 2000, pp. viii, 12–13). It appears that at this stage of analysis and mitigation strategy the government was approaching the cyber domain from a narrow, albeit specific, security-focused level such as espionage, while it considered more holistic approaches to cyber capabilities alongside surveillance, communications and 'data links between tactical units – for example aircraft and ships – to cooperate in combat with unprecedented speed and ease' (Department of Defence, 2000, p. 94).

Yet, a solid starting-point contribution from the 2000 DWP was to spark debate on cyber defence and cyber attack and to advance the notion that cyberwarfare is unlike traditional warfare. Further, it highlighted (briefly) that cybersecurity did have broad implications for defence and national security (also see Church et al., 2015, p. 38). Given the sustained increase in cyber activity targeting Australia and the benefits of attacker anonymity, this further led to the E-Security Initiative in 2001. This 2001 policy paper was focused on defending computer networks, preventing cyber espionage and safeguarding Australia's critical information infrastructure, which required 'a collaborative approach from the Australian Security Intelligence Organisation, Defence Signals Directorate [now the Australian Signals Directorate – the ASD], the Australian Federal Police and the Attorney-General's Department to assess and deal with identified threats' (Church et al., 2015, p. 38). Likewise, the 2000 DWP noted Defence's key role in combatting foreign interference and developing effective responses to cyber attacks against Australian Government infrastructure by an unknown adversary, but it did not explicitly name China itself (see Church et al., 2015, p. 38).

This budget for that year allocated aboutAU$2 million for reconfiguring networks, defending critical infrastructure and mitigating the theft of commercial intellectual property through cyber means (see D Williams, 2001). This dollar value quickly expanded in the following years, with

the 2002–2003 budget later committing AU$24.9 million over a four-year period for a cross-portfolio measure designed to improve the security awareness of critical infrastructure designated the National Information Infrastructure (NII; see Commonwealth of Australia, 2004). The NII acknowledged the nation-wide interconnection of communications networks and computers and defined these as 'information systems that support the telecommunications, transport, distribution, energy, utilities, banking and finance industries as well as critical government services including defence and emergency services' (Commonwealth of Australia, 2004). Yet, what would entail core 'battlespace' was ambiguous and remained problematical to define.

Meanwhile, it appeared that the E-Security Initiative was trying to kick-start a combination of policy methods to best guarantee the security of the NII by effectively utilising the Australian Security Intelligence Organisation (ASIO), the Defence Signals Directorate (DSD; now the ASD), the Australian Federal Police (AFP) and the Attorney-General's Department to best assess and deal with identified threats, in a whole-of-government approach to cybersecurity.

According to ASIO's (2002) annual report for 2001–2002, this approach involved:

- ramping up the production of assessments on infrastructure spending from 14 in 2000–2001 to 23 in 2001–2002,
- addressing demand for protective security advice,
- increasing the number of information technology companies being accredited, which was done through a joint program with DSD, from seven to 11, and
- technical 'sweeps' of sensitive venues. (p. 5)

This policy setting and the related template for prevention, preparedness and response translated into a direct resourcing increase in the number of technological and information-centric capabilities of ASIO and DSD and an intentional investment in capability requirements on the intelligence sector in general. Significantly, the ASIO (2002) revealed that the number of telecommunications carriers and carriage service providers being engaged in cyber incidents had multiplied as had the number of cyber attacks in the security sector owing to the vulnerability of the internet.

Further, the ASIO (2002) signalled in its 2002 annual report that it would continue to develop computer capabilities and that such developments might require a more aggressive

counterespionage posture as well (p. 7). Thus, at least at an operational level, the intelligence community was committing itself, and publicly, to increased involvement in the interception of data travelling both into and out of Australia, and consequently, funding for entities such as the ASD increased.

The ASD had announced in responses to parliamentary questions that in 2002–2003 it had received AU$2.13 million and that in 2003–2004 it would dedicate AU$1.92 million to installing equipment to develop forensic and incident response IT capabilities and OnSecure, an online IT security and incident reporting website for government agencies (see Commonwealth of Australia, 2004). OnSecure is a website specifically for government institutions for national reporting and alert systems, which operates alongside the Australian Computer Emergency Response Team's (CERT) national reporting scheme that provides targeted cyber assistance and advice to both the business community and government (see Rossi, 2003).

While this network security system created some overlap and added to dual security structures attempting to perform similar tasks, the OnSecure program was primarily created to replace existing report infrastructures within ASD and other government institutions, which were considered incredibly slow and outdated (Australian Signals Directorate, 2021). Importantly, the general manager of CERT at the time indicated that efforts would be made to liaise with the government to ensure data were not fractured and that the aim was to build international reporting mechanisms by working effectively together (Rossi, 2003). Thus, CERT would aim to operate alongside a network of information security experts to cohesive develop computer incident prevention, response and mitigation strategies.

Yet, it is significant that initial cyber-emergency reporting systems for both private and public enterprises were insufficient to adequately deter attacks and protect national industry, as indicated by the plethora of cyber incidents in the 2010s (see Chapter 3 for more details). This was not unique to Australia. For example, in the US, only 5% of industry partners surveyed proved capable of withstanding malicious cyber activity at the time (US Department of Justice, 2004). Moreover, the requirement for infrastructure entities to report incidents to governments in Australia in the early 2000s was voluntary (and very low) despite macro-style hacking and cyber attacks. This reporting issue was addressed in 2022 by requiring most critical infrastructure assets in Australia to comply with a mandatory cyber-incident reporting regime

within 12 or 72 hours of becoming aware of an incident (see MacPherson, Ludlow, Butler, Moore, Hilton, McGrath, Aquilina & Todd, 2023).

Regarding the AFP, the E-Security Initiative was also a broad measure that increased the outlay on capacity increase. The two main areas of the AFP that appeared to benefit at the time were the Australian High Tech Crime Centre and the AFP computer forensics department, areas of the AFP that received AU$2.0m in 2002–2003 and AU$2.4m in 2003–2004 (Commonwealth of Australia, 2004, p. 31943). Again, the focus was on malicious traffic.

Such investments were made to allow the AFP to host the Australian High Tech Crime Centre as well as to develop specific skills related to computer forensics and electronic evidence retrieval. At the time, these skills were largely devoted to crime-related cyber incidents (Commonwealth of Australia, 2004, p. 31943). Certainly, technology and its advancements had boosted cybercrime. However, the mechanisms mentioned, such as distributed denial-of-service (DDoS) or phishing have relevance in many forms of cybersecurity and are not solely unique to cybercrime. Importantly, in 2003, areas within the Australian High Tech Crime Centre were established in order to facilitate the provision of a coordinated national approach to multi-jurisdictional high-tech crimes, to improve the capacity to coordinate responses to high-tech transnational cyber attacks and to support national efforts to protect the NII (Commonwealth of Australia, 2004).

The AFP also established two teams to investigate high-tech crimes (based in Sydney and Melbourne) with the E-Security Initiative providing a platform to assist the AFP in intelligence sharing to respond to threats against the NII (Standing Committee on Communications, n.d.). The establishment of these units appears to be a seminal moment in approaches to fighting cybercrime in Australia, particularly by linking responsibilities to the NII and in its efforts to ensure greater coordination between policing and related organisations in the digital space (AFP, 2004, p. 12). For its part, at the time, CERT appeared much more definitive on the cyberthreats facing Australia. This included a security bulletin it issued in November 2000 that revealed explicit concerns about multiple worms likely to infect critical infrastructure systems, and other unique computer viruses that it had attempted to identify and describe (CERT, 2000). Ultimately, it appeared that the AFP was devoted to building capacity and providing information to help combat and deter online crime as well as to assisting with the new demands in order to enhance coordination between various organisations tasked with defending the NII.

Overall, the 2000 DWP was a solid but incomplete beginning to Australia's cybersecurity strategy. A criticism about it was that the Australian Government was still viewing Australian defence as mainly a beneficiary of a distinctive physical geography (see Church et al., 2015, p. 43). Yet as technologies developed, not only did kinetic warfare domains draw closer, but multilateral and transnational cyberwarfare (and cybercrime) domains were, in effect, already highly active and present (Dupont, 2015). In this sense, the 2000 DWP failed to adequately address the evolving importance of the need for greater situational awareness in the cyber domain and revealed the impotency of some early Australian Government strategic thinking, particularly on the subject of cyber deterrence in responding to state-based cyberthreats.

Thus, while there was promising growth in some areas of Australia's cybersecurity apparatus (and at least some early recognition of the growing importance of cyberthreats and appropriate responses between the government, including for policing, partner nations and the private sector), policy progress regarding cyber deterrence was still very slow and did not indicate the same levels of urgency and detail that other powers did—particularly allies such as the US (Goodman, 2010; Patacsil, 2014; Philbin, 2013; Wilner, 2019).

In this context, the 2000 DWP can be regarded as a starting point to developing and building cybersecurity and cyberwarfare capabilities in Australia. Conversely, the distinctive focus on cybercrime via the AFP and others has provided ongoing benefits in advancing threat detection and the coordinating of efforts of Australian law enforcement. These investments can be seen as later feeding to the development of areas such as attribution capabilities and also to the enhancement of capabilities against various transnational adversaries in order to 'observe, detect, disrupt or destroy' malicious networks (Standing Committee on Communications, n.d.).

Last, it should be noted that in May 2003, the then Chief of the Defence Force, General Peter Cosgrove argued:

> While it is likely that some type of crude kinetic effect will still be the ultimate expression of violence in war, it is also likely that as information and network-related war fighting techniques start to mature and to predominate, outcomes will be swifter, as dramatic and paradoxically less bloody than the classic force-on-force attritionist, paradigm of the past. (Waters, Ball & Dudgeon, 2008, p. 6)

Such open, public 'warfighting' statements by people like Cosgrove suggest the ADF was aware of the need to better develop and advance its capabilities of executing effective and

credible cyber-combat operations and of providing military support to national responses in a more complex digital environment that includes the cyber realm and the budding role of cyber deterrence to influence an adversary's behaviour.

2.4 Defence White Paper in 2009: Defending Australia in the Asia-Pacific Century

The 2009 DWP published under the Rudd Government elevated Australia's investment in cyber capabilities and reinforced their development as a security priority within a more pessimistic backdrop that focused on the prospective threat of the Chinese military. According to the government, 'The pace, scope and structure of China's military modernisation have the potential to give its neighbours cause for concern if not carefully explained' (Commonwealth of Australia, 2009, p. 34).

Significantly, this DWP explicitly stated that understanding the evolution of China's modernisation would be crucial, which implied that the modernisation was not an automatic cause for concern. However, it also stated that China must take the responsibility for explaining this modernisation to alleviate potential anxieties and mistrust in the Indo-Pacific region (Commonwealth of Australia, 2009, p. 34). The then Minister for Defence Joel Fitzgibbon also wrote in the preface that although Australia reaffirmed its commitment to the alliance with the US, China was challenging US primacy and that Australia was focused on the potential threat from the rise of Chinese military power (Commonwealth of Australia, 2009, p. 9).

In addition, in this context, given the view that China could be more assertive in its behaviour and actions, Australia would recommit resources to a new strategic focus on China that incorporated long-range strategic assessments, albeit without an explicit or definitive forecast. Although the DWP

> did not predict any imminent decline of the US military power, it did, however, identify the economic rise of new regional powers (namely, China, Japan, India and Russia) and their likely challenge to the US supremacy. As a result of the redistribution of economic power, the White Paper forecast the balance of strategic power in the Asia-Pacific to gradually shift in the challengers' favour and the likelihood of 'strategic competition' amongst them. (Tubilewicz, 2010, p. 151)

This singling out of China as the most significant challenger was founded on several threat perceptions, including in the cyber realm because of

> China's increased espionage activities and cyber-warfare attacks against the Australian government, allegedly including electronic spying against Prime Minister Rudd himself, in addition to targeting over the past several years expatriate Chinese within Australia, Australian businesses, and sources of both commercial and strategic technologies. (McCaffrie & Rahman, 2010, p. 66)

In describing Chinese cyberthreat behaviour and trends, cyberwarfare and related aggressive actions were regarded as an emerging area of defence and security/intelligence interest, as was the increasing risk of cyber attack to both the Australian Government and private-sector networks. The growing importance of critical infrastructure services and combative activities in the cyberspace was built, in part, upon the 2008 E-Security Review, which had effectively found that Australia's cybersecurity development was deficient, had poor capabilities and had insufficient resourcing to deal with potential security flashpoints. For instance, in response to an increasing reliance on networked operations, the 2009 DWP established the CSOC, which has been designed to address national responses to cyber incidents across government and critical private-sector systems. It also established CERT to provide the government with enhanced cyber-situational awareness and more agility to facilitate operational responses to cybersecurity incidents (Commonwealth of Australia, 2009).

Indeed, a core purpose of the 'whole-of-government' 2008 review of cybersecurity settings was to develop a contemporary policy framework that prioritised mitigation in order to keep pace with rapidly expanding cyberthreats. This framework included providing cybersecurity alerts and creating a secure, trusted electronic operating environment for both public and private sectors, and was tasked to the Attorney-General's Department ('Govt Launches Review of e-Security', 2008). The backbone of the review was that the government's e-security policy at the time continued to be informed by the E-Security National Agenda established in 2001 that had been partly reviewed in 2006 to identify intrusions, invest in operational resilience and gain a resilience edge in the cyberspace domain (see Ruddock, Coonan, Nelson, & Nairn, 2006).

Yet, in terms of the scope of cyber-deterrence positioning, all these policy papers had major gaps and were short on thinking and language and even retaliatory assumptions related to active

cyber deterrence and cyber deterrence by punishment. Instead, these papers were principally focused on ensuring mitigation, implementing passive deterrence, detecting anomalous actions and providing technical 'best-practice' guidance for protecting against activities that could affect critical networks. Although these aspects are certainly important, if a defender is only focused on denial, skilled attackers will always inevitably successfully compromise them (Van de Velde, 2023).

When the 2009 DWP did address the potential impact of cyberwarfare, it was in the context of a broad range of contingencies that could 'potentially be compromised by cyber-attacks on our defence wider governmental, commercial or infrastructure-related information networks' (Commonwealth of Australia, 2009, p. 83). Thus, policy thinking at the time appears to be absorbed in deterrence-by-denial efforts, and it was concluded that 'the main role of the ADF should continue to be an ability to engage in conventional combat against other armed forces' (Commonwealth of Australia, 2009, p. 22). Meanwhile, the policy about how to best integrate cyber deterrence with a more traditional muscular defence posture aimed at China remained uncertain.

Nonetheless, as mentioned, the Rudd Government did establish the CSOC in 2009, an internal department of the DSD with the broad mandate to provide greater situational awareness and respond to cyberthreats. The CSOC is dedicated to analysing cyberthreats, coordinating a cohesive government response and developing whole-of-government strategies with a renewed focus on the resilience of vital infrastructure (see Faulkner, 2010). Hence, the Attorney-General's Department took the central lead with the aim of creating a code of practice and providing enhanced cyber-situational awareness, protective monitoring and threat/ vulnerability management, which included the consideration of the roe of national and international law to deal with cyber attacks (Faulkner, 2010).

Consequently, in addressing evolving networked systems, the overriding concern was criminality and the assessment was that 'the production, scale and distribution of malicious code has become a prolific criminal industry, making malware stealthier, more targeted, multifaceted and harder to analyse and defeat' (Attorney-General's Department, 2009 p. v). The Attorney-General's Department (2009) strongly emphasised the threat of electronic intrusions into Australian networks and, in particular, in the banking and finance and the commercial sectors (p. v). Meanwhile, the 2009 DWP had a broad strategic consequence as it perceived cyber attacks and cyberwarfare as a reality, and acknowledged this by discussing

various cyber scenarios that could also involve defence and military planning (Department of Defence, 2009 p. 83).

In sum, in the 2009 DWP, the Rudd Government acknowledged the multifaceted nature of the cyber domain, the increasing reliance upon this domain from both the public and private sectors and the need for coordinated security and defensive efforts in this domain, although it predominantly focused on legal issues and on deterrence by denial and largely overlooked deterrence-by-punishment processes and mechanisms.

In 2011, Australia again appeared to be proactively engaging with international partners in the area of cyber preparedness, as illustrated in its talks with the US that confirmed that the ANZUS Treaty could be invoked in response to a cyber attack (US Department of State, 2011). In other words, cyberspace would be an additional ingredient of the mutual defence treaty, which means that a cyber attack on one state actor could lead to a response by both nations. Then US Defense Secretary Leon Panetta stated, 'I think it's in large measure a recognition of what I've been saying time and time again, which is that cyber is the battlefield of the future' (Stewart, 2011).

Building on such rhetoric and collective security framing, the inclusion of cyber is significant to Libicki's framework that questioned not only whether a nation-state's response to a cyber incident was proportionate but also whether its actions would send the 'right' message to allies and whether other third parties could become involved beyond any immediate cyber incident and its context, which will be addressed in detail in Chapter 5. At the very least, the 2011 talks did share reflections about common cybersecurity requirements in due diligence although also extending a diplomatic olive branch to China by desiring 'a positive, cooperative and comprehensive relationship with China', potentially with a view to avoid escalation into a full-scale war (Department of Foreign Affairs and Trade, 2011).

Yet, although the 2011 talks did not explicitly tie cybersecurity commitments to declarations of war, the one combined statement emphasised mutual security obligations under the ANZUS Treaty and shared concerns about cyber difficulties. Moreover, the communique is unique for its time, compared with the 2010 and 2012 communiques for Australia-United States Ministerial Consultations, in that it is the only such document to have a clear-cut section defining cybersecurity concerns in the event of a computer-related attack and a deliberate commitment to cooperation between Australia and the US that extends into the virtual space (see Department of Foreign Affairs and Trade, 2010, 2011, 2012). The 2011 announcement is

particularly significant for Australia and the US as it is the first time that the US extended such a commitment in the cyber domain outside of the North Atlantic Treaty Organization (NATO; DFAT, 2011).

Alongside these international alliance developments, there were domestic policy developments to broaden defence and security postures related to the cyber domain. In 2010, the CERT was formally promoted as a government institution, building on the work of the Australian Cyber Emergency Response Team, AusCERT, established in 1993 at the University of Queensland (Department of the Prime Minister and Cabinet, 2016, p. 30). CERT was regarded as 'the single point of contact for cyber security issues affecting major Australian businesses' (Department of the Prime Minister and Cabinet, 2016). It was also part of the ACSC, and it shares information and works closely with the ASIO, the AFP, the ASD and the Australian Crime Commission (Australian Government Directory, 2021). In this context, establishing CERT could be viewed as critical to the civilian incorporation into cybersecurity in Australian policy planning.

However, as mentioned, despite the realisation that the private sector would require extended assistance in cybersecurity, the monitoring and reporting of cyber incidents remained voluntary in nature. Indeed, the former Gillard Government established a 'Top 4' mitigation strategy in order to assist in moderating cyber intrusions, which promised to alleviate 'at least 85% of the intrusion techniques that the Cyber Security Operations Centre responds to' (ASD, 2013). Certainly, such matters are important to developments in Australian cybersecurity and associated defence settings, but the glaring omission to this point was still a reactive and passive framework.

In January 2013, the ACSC was announced and headquartered in the ASD, and it was to comprise 'capabilities from ASD, ASIO, AGD, AFP and the Australian Crime Commission' (Brangwin & Portillo-Castro, 2019). The ACSC would build on the existing work in CSOC and ASD and was expected to continue to play a primary role in their cyber operations as the core hub for greater collaboration and information sharing to combat the full range of cyberthreats (Parliamentary Standing Committee on Public Works, 2017). As then Prime Minister Rudd (2013) asserted:

> Australia now operates in a world of complex systems, all vulnerable to malicious cyber activity, whether originating from states, criminal organisations or misguided individuals.

> For this reason, the Australian Government's determination is to continue to lift our cyber capabilities including our network defences. This Centre will bring together the existing cyber capabilities from across Defence, the Attorney-General's Department, ASIO, the Australian Federal Police and the Australian Crime Commission. These capabilities will include ASIO's cyber espionage specialists, experts from the Australian Signals Directorate's Cyber Security Operations Centre.

The creation of the ACSC formalised the coalescence of many different department capabilities and marked the commencement of rethinking about the Australian Federal Government's tools for identifying cybersecurity weaknesses and addressing problems in the wider defence of the country's cyber domain. Arguably, it also signalled to potential adversaries such as China that Australian cyberwarfare capabilities were being more fully apprehended and that the scope of various government bodies would entail responses to address and mitigate cyber incidents.

Overall, under Rudd and Gillard, the focus of 'whole-of-government' and allied cybersecurity remained on deterrence-by-denial efforts in attempts to detect and mitigate unlawful access and espionage, cybercrime and the related damage to the integrity of critical electronic networks from cyber incidents. The 2009 DWP also lacked a clear definition of the malicious actions that would constitute a cyber attack and would result in some form of retaliation. However, the need to improve offensive capabilities and to communicate the extent of Australia's cyber abilities and a more proactive domestic strategic approach came to the fore when then Prime Minister Malcolm Turnbull announced the release of the 2016 Cyber Security Strategy.

2.5 Australia's 2016 Cyber Security Strategy and Defence White Paper

In 2016, the then Turnbull Government made many key announcements that would drastically change the government's approach to cybersecurity, cyberwarfare and cyber deterrence. In short, cyberspace was presented as a fundamental 'point of friction' in the backdrop of geopolitical tensions (Department of Defence, 2016, p. 43).

A media release by Former Prime Minister Malcolm Turnbull stated that the Cyber Security Strategy would deliver improved cybersecurity

> through 33 new initiatives, supported by over $230 million in Australian Government funding directly resulting in more than 100 new jobs to boost the Government's cyber security capacity and capabilities. This investment complements the $400 million over the next

> decade – and roughly 800 specialist jobs – the Government has committed to improve Defence's cyber and intelligence capabilities through the 2016 Defence White Paper (Malcolm Turnbull, 2016).

In terms of key initiatives, the 2016 Cyber Security Strategy was strong on expanding the scope of ASD and incorporating not only analysis and detection of malicious threats, but also a commitment to boost the capacity to respond to cybersecurity threats with both offensive and defensive means, although it did not reveal much actual detail on Australia's cyber posture and how its cyber capabilities would be allocated and implemented for both offence and defence (Department of the Prime Minister and Cabinet, 2016, pp. 6–7, 28). Nonetheless, the paper proposed multiple significant adjustments by the Australian Government, ranging from reforms to the ASD to hiring experts for increasing Australia's skillset to 'cyber'. These adjustments were prioritised in order to build the nation's defence capability to support the defence-related strategies of the ANZUS alliance related to advancing cyber norms and a rules-based global order (Commonwealth of Australia, 2016, pp. 2–3). Feakin argued that 'overall, this White Paper is impressive, presenting a costed spending plan to fund the commitments made (2016). A positive step is that "cyber security" has its own dedicated spending line, with a commitment to spend $300–$400 million'.

The Turnbull Government's prioritisation of a 'rules-based global order' in 2016 was captured in the creation of a new role of Cyber Ambassador, that is, an individual committed to identifying opportunities for international cooperation and ensuring that Australia had a coordinated voice on international cyber issues (Department of Foreign Affairs and Trade, 2017b). The purpose of this new position was to lead Australia's whole-of-government international engagement with allies to 'advance and protect Australia's national security, foreign policy, economic and trade, and development interests in cyberspace and critical technology', despite the consequences of a 'global' cyberwar being highly indeterminate (Department of Foreign Affairs and Trade, 2017b, p. 7).

This role also found increasing significance in the review of pre-existing treaties such as ANZUS and was expanded to include mandates such as all technologies deemed 'critical'. This expansion increased its scope and further illustrated the importance that Australia places on the profile of its cybersecurity industry and on the sharing of technology and expertise in allied relationships (Shrimpton & Cave, 2021). Nevertheless, the position of Cyber Ambassador appeared to be primarily aimed at providing a 'diplomatic edge' to countering Chinese threats,

as Australia turned to more transparent and open public engagements and statements to counter the growing Chinese cyber aggressiveness.

Perhaps a most significant fact was that Turnbull had confirmed that Australia had a 'significant' offensive cyber capability. Turnbull later added that the 'use of such a capability is subject to stringent legal oversight and is consistent with our support for the international rules-based order and our obligations under international law' (Malcolm Turnbull, 2016). Given the changing character of warfare, Turnbull announced the development of these offensive cyber capabilities of the ASD and the willingness of the government to deploy them by asserting that 'this offensive capability adds a level of deterrence, it adds to our credibility as we promote norms of good behaviour on the international stage and, importantly, familiarity with offensive measures enhances our defensive capabilities as well' (Karp, 2016). Further, it was the first such acknowledgement that cyber attacks could directly jeopardise ADF's warfighting ability (Department of Defence, 2016, p. 40).

The 2016 DWP was highly different from prior cyber announcements by going on the offensive in compromising national security and signalling that offensive cyber capabilities could be used to deter possible attacks. As already discussed in this chapter, all previous cyber announcements were more about ensuring mitigation and resilience, securing Australian cyberspace and prioritising defensive measures. However, as also noted, the 'red line' or threshold for a retaliatory response by Australia to a cyber attack was not publicly stated, especially since once cyber weapons are revealed, the vulnerabilities they rely upon can be patched, rendering them redundant (Seligman, 2022). In addition, the specified cyberthreats and challenges included organised criminal syndicates and foreign adversaries rather than China, which was not explicitly labelled per se. Nonetheless, the strategy proposed investments to enhance operational capacity—presumably to support attribution as well—and placed the ASD at the front and centre as the key cyberwarfare development institution for the Australian Government (see Coyne, 2016).

Overall, the 2016 DWP can be considered a fast-tracked operational uptake in 'prevent and disrupt' actions as well as in separate actions for the prospect of extended cyberwarfare operations. As Turnbull highlighted, Australia's offensive security capabilities would now be seen as a top-end requirement, given that Australia's 'defensive measures may not always be adequate to respond to serious cyber incidents against Australian networks … an offensive cyber security capability housed in the Australian Signals Directorate provides another option

for governments to respond' (Pauli, 2016). Thus, active deterrence appears to have been extended to allow the option to confront state-based adversaries via the ASD.

Accordingly, a mix of defensive and offensive cyber capabilities were promoted in 2016 as essential components of cyber awareness and risk assessment and for shaping international behaviour. Although lacking in detail, the public announcement and communication of offence capabilities can be seen as part of signalling an intent, which is an essential component of any deterrence strategy. The promise of offensively targeting malicious actors was a deliberate warning sign to all real or potential adversaries, including China. In other words, 'specific reprisal actions need not be explicitly threatened to contribute to deterrence' (Libicki, 2017, p. 46).

Of course, offensive cyber operations also all carry many risks. These were unresolved in the 2016 DWP and would still need to be carefully considered. For instance, 'for cyber operations in support of the ADF, as with conventional capabilities, the commander must weigh up the potential for achieving operational goals against the risk of collateral effects and damage' (Hanson, F & Uren T, 2018, p. 8).

Hence, again, there were unresolved political and legal issues surrounding the identification of the target, the specific circumstances under which this offence posture might surface and the methods to be used. These issues included ensuring the proportionality of the response to the attack and to the advantage gained, and related proactive steps (see Bloch, Peach, & Peake, 2018). However, ASD's legislative and oversight framework allows the scope for technological improvements; for example, Section 7(e) of the *Intelligence Services Act 2001* authorises ASD 'to provide assistance to Commonwealth and State authorities in relation to … (ii) *other specialised technologies*' [italics added for emphasis]. Moreover, deterrence calculations 'necessarily presume a high order of rationality and calculability. When the subject is cyberspace, it also requires a mindset capable of inferring effects and costs from threatened cyber-attacks' (Libicki, 2017, p. 47).

At the very least, building Australia's offence capability would demand continual risk assessment and planning along with stable investment. Further, proportionality and attribution would require investments of time, while disproportionate responses could trigger an escalation especially if spilling across multiple networks. As Libicki asked, '*Will others join the fight?*' becomes an increasingly serious question in offensive calculations due to having a

multiplicative effect on the complexity of actors and systems involved. In addition, as Libicki noted (2017), the requirements for 'acceptable' and well-communicated

> thresholds as well as for credibility have been part of deterrence theory since its inception. Furthermore, the notion that certain types of punishment cannot be credibly threatened if they are disproportionate to the crime has been well understood in the literature on nuclear deterrence. The difference here is that using cyber-attacks for punishment raises issues whose considerations are not so salient in other domains. (p. 45)

Moreover, as Ford (2018) asserted, it would remain important in any Australian context that those government agencies tasked with managing national security in cyberspace 'consistently act in a trustworthy manner. Hence, there should be guarantees that decisions related to cybersecurity oversight and governance are not driven by short-term political gains'. At the time of writing, information about how Australia would actually assess the consequences of acting offensively in the cyber domain against an actor such as China remains classified.

Even so, given the lack of offensive precedents and the efforts to improve intrusion analysis capabilities under Turnbull, the ASD would be positioned not only to play a central role in reprisal and punishment capability but also to assist the corporate sector to resist and analyse cyber intrusions (see Crozier, 2018). The general aim was for cybersecurity to be improved via ASD's assessment of vulnerabilities, its provision of technical security advice and the implementation of public- and private-sector cybersecurity awareness programs, which were all designed to 'uplift' cybersecurity skills among unskilled workers in the cyber domain and build resiliency to lower-level cyber attacks such as phishing (Crozier, 2018). The ACSC would then endeavour to deploy high-speed responses to serious cyber incidents (such as ransomware) to facilitate a 24/7 capability for addressing cyber problems, given that the effects of many cyber attacks can be relatively restricted and narrow (see Coyne, 2018).

Another overlapping key announcement by Turnbull in 2017 was of the creation of an Information Warfare Division (IWD) under the Joint Capabilities Group within the Department of Defence (see Coyne, 2017). In broad terms, the IWD would aim to help to develop information warfare capabilities for the ADF, ideally enabling the ADF to 'be able to control and influence the information domain during conflict and pre-conflict phases' (see Tehan, D, 2017). Yet, the type of cyber action that will constitute an act of war remained unclear.

However, one notable aspect of the IWD is that it would likely only be involved in enhancing the ADF's ability to operate effectively in the information environment and in assisting military operations as a supporting force to kinetic warfare operations (with operational and tactical-level effects). Therefore, it would not necessarily feature heavily in Libicki's (2009) defined 'strategic cyberwar', as its purpose seems primarily aligned with self-defence and passive defence in protecting military systems and with areas such as cyber training and cyber awareness. However, for some, the overriding 'cyber as an enabler' concept remained too constricted and limited. The ADF approach to cyber

> is based on understanding cyber as an enabler to other domains rather than a domain in itself. As enabler, cyber sits with communications and logistics as a requirement for each single-service; each service has its own unique terrain, requirements and priorities and therefore must generate its own enabling capabilities. (Australian Army Research Centre, 2019)

At the very least, it can be argued that it is highly unlikely that the integration of ADF cyber into any 'whole-of-government effort' would not automatically flow into a more strategic and open-ended cyberwar template. In fact, the Department of Defence itself clarified that 'in the Information Age, if you control the opponent's information environments through coordinated and integrated influence campaigns, cyberwarfare and electronic warfare, then you control your opponent' (Defence Science and Technology Group, 2022). The logic implies that even if the IWD does not fully undertake the active defence and offence approach listed above, it is certainly a stated desired approach from the entire Australian Government's cyberwarfare architecture, such as ASD, ACSC and other intelligence agencies and military entities, as stated in the 2016 DWP (Commonwealth of Australia, 2016, p. 88). These are all integrated governance facets of a deterrence architecture that the Australian Government can refer to, and employ, for potentially authorising offensive cyber operations against adversary states.

Hence, with accelerating changes in both geopolitics and technology, the 2016 Cyber Strategy was closely aligned to the DWP (also released in 2016), which touched on cybersecurity although it could have 'engaged in a more holistic discussion across the spectrum of cyber capabilities' (Feakin, 2016). Nonetheless, the DWP 2016 also stated that cyber attacks were 'a real and present threat' and identified key areas for more cooperation in efforts to strengthen defence systems and networks alongside personnel in a generally deteriorating geopolitical situation (Department of Defence, 2016, p. 18). It highlighted that while a major conflict between the US and China was viewed to be unlikely, cyberspace remained both a highly

contentious public and private space and pointed to the ubiquitous nature of cyber attacks (Department of Defence, 2016, p. 7).

Another particular point worth noting from the 2016 DWP is about public–private partnerships and a focus on the business and Intellectual Property aspects of cybersecurity, which again might be interpreted as an early warning statement to actors such as China who had been accused of stealing technologies via cyber means (this issue will be covered in more detail in Chapter 3). In this context, the 2016 DWP reinforced that maintaining Australia's 'technological edge and capability superiority over potential adversaries is an essential element of our strategic planning. The capability superiority that Australia has traditionally maintained in the wider region will be challenged by military modernisation' (Department of Defence, 2016, p. 16).

Certainly, the growth in the capability of China's military forces could be seen as the most predominant example of regional military modernisation that propelled key Australian posture and force structure decision-making as well as international cyber-engagement efforts (see Shugart, 2021). Perhaps the most unequivocal paragraph inferring to China in the 2016 DWP was as follows:

> While it is natural for newly powerful countries to seek greater influence, they also have a responsibility to act in a way that constructively contributes to global stability, security and prosperity. However, some countries and non-state actors have sought to challenge the rules that govern actions in the global commons such as the high seas, cyberspace and space in some unhelpful ways, leading to uncertainty and tension (Department of Defence, 2016, p. 45).

Cyberthreats from China will also have effects well beyond the ADF, with the potential to attack other sectors of Australia's economy and critical infrastructure. Consequently, for the whole-of-government' strategy to work effectively, it would need to entail effective public–private collaborative partnerships to prepare for future events.

Again, the ACSC would remain critical to ensuring that private enterprises have a greater ability to protect economic and commercial information. This is noteworthy when examining the cyber relationship between China and Australia. It has been argued that China's cyber policy places significant emphasis on extracting large amounts of sensitive information from various nations and in various domains, but their economically motivated cyber espionage has

been a significant trouble point for Australia and other allied nations (see M Payne et al., 2021). Indeed, former FBI Executive Assistant Director Shaun Henry asserted that 'there are two types of companies: companies that have been breached and companies that don't know they've been breached' (McConnel, 2010). Such assessments continue to place significant pressure on defence and other organisations tasked with dealing with Chinese cyber intrusion—and the ACSC's capabilities will play an important role in driving deterrence calculations and objectives.

For instance, in analysing Australia's deterrence capability in the cyber domain, many questions revolve around how clearly Australia communicates capability and intent to any potential aggressor such as China to, hopefully, consider whether any of its cyber operations are proportional to any advantage gained. Therefore, statements such as that of the Turnbull Government that the ACSC would be transitioning to a 24/7 response capability to deal with global ransomware attacks such as WannaCry pushed Australia into a 'permanent' state of readiness to address and respond to ongoing and persistent cyberthreats. In engaging with targets that may not be reachable using conventional capabilities, this statement marked the first time that the Australian Government had identified a specific federal body that could be approached at any time by Australian entities and that these entities would have access to federal resources deployed on their behalf such as upgrades, patches or configuration changes.

Indeed, tactical victories, even of a purely digital nature, can affect strategic-level decision-making and thus communicating Australia's capability in terms of timing and power projection can add to the effectiveness of deterrence (also see Harold et al., 2016). In short, Australia under Turnbull had

> announced that it has an offensive cyber capability that it is prepared to use against offshore cybercriminals and terrorists, and to support military and law enforcement operations. Close attention needs to be paid to the ways in which these capabilities are communicated, to avoid any potential for confusion and misperception about how these capabilities will be used (Miralis, 2021).

Interestingly, the breakdown of capability tasks appeared to indicate that institutions such as the ACSC and CERT would remain the central points of contact for the private sector and would utilise strategies developed by the ASD (Department of Defence, 2016, pp. 24–25). The ASD itself was housed within two significant chains of command. First, there was the civilian-comprised ASD that fit into the aforementioned passive cyber-defence framework. Second,

there was the IWD, the military arm of cyber defence to integrate cyberwarfare, electronic warfare and influence operations into a single information capability (Hanson & Uren, 2018).

However, by 2017 progress was stalling to some extent and was not always even. The Auditor General's office report in 2017 had troubling findings regarding cyber defences in many government departments (Australian National Audit Office, 2017, pp. 8–9). Of the three departments investigated—Department of the Treasury, National Archives of Australia and Geoscience Australia—all were found wanting in the protective levels of cybersecurity and adherence with publicly stated government standards (Australian National Audit Office, 2017). The standards against which these departments were held are the top four recommended mitigation strategies: application whitelisting, patching applications, patching operating systems and minimising administrative privileges (ASD, 2013). Notably, the ASD advised that if the government bodies had implemented the above four strategies it could have prevented 85% of targeted cyber intrusions (and this number has been reinforced by ASD multiple times; ASD, 2013, 2020).

Last, it is worth noting that in 2018, the regulation of critical infrastructure under the *Security of Critical Infrastructure Act 2018* (the SOCI Act) aimed to place stricter cyber-reporting obligations on these entities, such as the electricity, communications, data storage or processing, financial services and markets, health care and medical, and the defence industries. Then, in March 2022, the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 was passed with the aim of strengthening the resilience of critical infrastructure by expanding the sectors to which the SOCI Act was applicable. Part of what inspired this expansion is in the Optus and Medibank breaches, which are covered later in this chapter. Thus, the SOCI Act aimed to add to Australia's deterrence-by-denial capabilities.

2.6 Australia's Cyber Security Strategy 2020

In 2020, Australia issued a new Cyber Security Strategy under Morrison that interchanged with, and extended from, the 2016 strategy. The strategy laid out an ambitious purpose and engagement across a spectrum of priorities and aimed for 'a more secure online world for Australians, their businesses and the essential services upon which we depend' (Department of Home Affairs, 2020, p. 6).

As with the previous white papers, the 2020 strategy began with an analysis of the threat environment and stated that ‘nation states and state-sponsored actors seek to compromise networks to obtain economic, policy, legal, defence and security information for their advantage’ (Department of Home Affairs, 2020, p. 12). Moreover, as under Turnbull, the 2020 DWP did not unambiguously name any particular problem nation-states, including China, but instead relied on repeating terms, such as the challenges from generic ‘state-sponsored’ actors (Department of Home Affairs, 2020, p. 6, 12).

Thus, the 2020 DWP continued a running theme in various high-level government documents that continually refer to nation-states, cyber attacks and cyberspace as an operational domain, but it did not give detailed threat representations. Yet, China, in particular, had been frequently identified by numerous other states, including the US and the United Kingdom (UK), for deploying its cyber weapons in the pursuit of cyber destabilisation and for its efforts to obtain competitive economic and commercial edge, part of what was identified in Chapter 1 as ‘rob, replicate and replace’ (see Dorfman, 2021). In a networked world, at the DWP level at least, it was apparent that the Australian Government in 2020 was still highly reluctant to directly ‘name and shame’ China as a potential adversary nation without allied support. It is possible that this was to prevent escalation between the two states. However, this mentality eventually was dismissed, culminating in Australian intelligence agencies in 2023 joining US counterparts in blaming the Chinese for the largest theft of intellectual property in history (Macmillan & Green, 2023). This issue will be discussed in detail later in Chapters 2, 3 and 4.

Still, the Morrison Government was clearly concerned with state actors engaging in the cyber domain and increased federal spending on cybersecurity ‘to $1.664bn, including initiatives to boost community awareness and preparedness and helping critical infrastructure providers assess vulnerability in their networks’ (Auckburally, 2020). These initiatives included additional funding for the AFP to investigate and counter cyberthreats, a public awareness campaign, and measures fortifying small and medium businesses, universities and households (Sadler, 2020). The investment period was set as 10 years, and the investments were strongly pointed at areas such as critical infrastructure, investigating cybercrime, stronger defences for government networks and data, strong guidance and a 24/7 hotline for cybersecurity advice (Department of Home Affairs, 2020, p. 6). Despite this being Australia’s largest ever investment in cybersecurity, none of those commitments was completely new, not even the idea of a 24/7 hotline. More than AU$12 million was allocated for ‘new’ strategic mitigations

and active disruption options, aimed at enabling ASD (and major telecommunications providers) to prevent malicious cyber activity (e.g. by blocking known malicious websites at speed), which Turnbull had also mooted.

Building off this concern for combatting cyberthreats and enhancing options for understanding malicious cyber activity, more than AU$62 million was also directed to support a more robust situational awareness capability—attribution—to better enable ASD to understand and respond to cyberthreats on a national scale. This was to be coupled with advice and assistance about ways to mitigate cyberthreats via public–private partnerships (Department of Home Affairs, 2020, p. 12). Overall, the 2020 paper appeared to place far greater emphasis on attribution, expanding the cybersecurity workforce and being able to block emerging threats in 'near real-time' (see Uren, 2020). The 2020 strategy appeared to be 'much more robust from an enforcement and deterrence perspective' (Uren, 2020). The paper itself explicitly stated the intention to incorporate deterrence into the strategy, emphasising:

> We work to actively prevent cyber attacks, minimise damage, and respond to malicious cyber activity directed against our national interests. *We deny and deter* [emphasis added], while balancing the risk of escalation. Our actions are lawful and aligned with the values we seek to uphold, and will therefore be proportionate, always contextual, and collaborative. We can choose not to respond. (Department of Home Affairs, 2020, p .26)

Thus, the 2020 strategy was in many ways a steady continuation of the previous cybersecurity strategy, but also, it did build on the emphasis of using deterrence within threat-sharing platforms and the technological advancements in dealing with the more aggressive elements in the cyber domain. It acknowledged that state-based contest was part of any cyber framework for understanding and responding to cyberthreats and hence differed from the 2016 strategy, which referred particularly to espionage and related criminal and non-state transnational elements of cyber operations. The intention of the Australian Government in stating 'we deny and deter' was clear and certain: Australia could now could do much more than just identify cyberthreats, and the ASD would not only know 'who did it' (see Chapter 5) but also in what way the attack could best be stopped.

The Morrison Government also proposed, in part, to address how Australia would adapt to cybersecurity and cyber deficiencies. This incorporated the acknowledgement that most data in Australia are stored by private enterprises, and therefore, 'Australia will not be secure until all businesses take steps to protect themselves, their supply chains and their customers'

(Department of Home Affairs, 2020, p. 28). It stated that the government would establish partnerships with critical infrastructure operators to shore up cyber defences that crucially, involved the political will to 'actively defend networks, using both offensive and defensive tools' (Department of Home Affairs, 2020, p. 28). Hence, all critical infrastructure operators were expected to take 'reasonable' steps to ensure robust cybersecurity. It was also reported that Australia would recruit 500 'cyber spies' and build its offensive capabilities to take the online fight overseas (see Galloway, 2020).

Further, Morrison stated that the threshold of evidence to attribute an attack to a particular country publicly was 'extremely high' but declined to name China (Hurst, 2020). Importantly, the strategy did signal the use of offensive tools to deter sophisticated state-based cyber hacks. The implications were that if a state such as China targeted Australia's critical infrastructure through cyber means, regardless of whether the infrastructure was privately owned or not, the Australian Government would treat it as a strategic asset and act to defend, deter and possibly deny further intrusions.

As already stated, deterrence rests heavily on perceptions and discernments and has a psychological effect. Therefore, while stability in cyberspace is difficult to predict, effective cybersecurity is about more than attribution and technology advancement per se. Nevertheless, the 2020 DWP could have attempted to deliver a firmer, ore clear-cut warning to China in attempting to influence its strategic observation and calculations regarding Australia and to deter a systematic institutional cyber attack by China.

For instance, it might be somewhat confusing for observing foreign adversaries to note then Minister for Home Affairs Peter Dutton's rather inward-looking emphasis on how the 2020 strategy granted expanded domestic powers, such that 'If you're a pedophile [sic] you should be worried about these powers' (Stilgherrian, 2020). It could be argued that the high-profile ministers responsible for 'pitching' these documents remain an essential component of deterrence communication, and hence, confusing the matter with domestic politics or glib political point scoring might not be helpful in attempts to influence China's strategic decision-making.

In general terms, the DWP framework and associated political cues and signalling component can be seen as haphazard and incomplete. Alternatively, it has been argued that an effective cyber strategy must have consistency and needs to address

> missing answers relating to the *how* and *what*. Some statements in the strategy are effectively placeholders indicating that details will be determined at a later stage. In addition, the measures for success are imprecise. In most cases, an improvement larger than 0% can be interpreted as a win. Precision, clarity of execution, and metrics need to be better articulated for the strategy to make the desired impact (Yip, 2020).

While it can be difficult to pinpoint for diplomatic and political reasons, such a lack of precision might also undermine the deterrence-by-punishment posturing when stipulating its offensive cyber operations. Even approximate terms related to the 'scope of potential targets' that the government would willingly consider in cyber deterrence could conceivably manipulate the cost–benefit analysis of an adversary, as observed in US threats against Russian energy grids in 2019 (see Sanger & Perlroth, 2019).

Similarly, the 'name and shame' approach might have been too extreme for the Morrison Government to consider, but something more specific such as advancing on the 2016 assertion of the targeting of international criminal networks could have been a more assertive and forceful tool for the Australian Government to consider. The government could have reveleaed that Australia and Australian entities have been targeted by criminal actors operating from China and implied that if the Chinese government is unwilling or unable to help with deterring these criminals, the Australian government will carry out its own deterrence operations and actions.

Specifically identifying APTs might have been an especially interesting tactic as once these entities are publicly identified, there is typically geographic attribution applied as well as a geographic naming relative to location—such as the infamous 'Putter Panda' (see Section 3.7.2 - PLA Unit, 61486). The inference again would be that Australia knows 'who did it' and its deterrence strategy does not need to be specific on the 'how', as this can undermine efforts. Nevertheless, a well-defined statement of intention and 'what' could be beneficial to deterrence-by-punishment ideas.

Nonetheless, where the 2020 Cyber Strategy did appear to make a positive contribution to deterrence strategy is the boosting and reorganisation of cybersecurity infrastructure and related mandates (Department of Home Affairs, 2020 pp. 39–40). In particular, it confirmed that cyber actions against Australia would still have to contend with the ASD. As Director-General Rachel Noble (2020) noted in an address, the ASD 'is both the poacher and the gatekeeper. Both sides of our brain work together to protect ourselves from people like us'. In

addition, while some secrecy of course remains to protect ASD's operations, Noble (2020) also explicitly stated that the ASD, a body already authorised to conduct offensive operations by former Prime Minister Malcolm Turnbull, was conducting operations with the intent of pilfering capabilities from potential adversary states. Noble (2020) also conceded there was a need for the ASD to be transparent about 'what' it does, but 'not how it is done'.

This quotation is highly informative about the difference of how deterrence often occurs in the cyber domain from the physical domains—entities do not assert how they will deter adversaries, but rather, they allude to the possible effects of deterrent actions. It is even possible that Noble may even be indirectly referencing Sun Tzu here: 'If you know yourself but not the enemy, for every victory gained you will also suffer a defeat' (Tzu, 1963). At the very least, in terms of China, Sun Tzu still influences its military's strategic thinking, which will be discussed in detail in Chapter 3. Here at least, the concept fits neatly with ASD's defined mission: to reveal their secrets, and protect our own (ASD, 2022).

In short, the 2020 Cyber Security Strategy focused on improving the resilience of Australia's critical infrastructure, enhancing the cyber defences of private enterprise through government engagement and increasing the capability and offensive operations of the intelligence sector. A significant amount of funding and initiatives labelled in the action plan were directed at federal law enforcement agencies such as the AFP and the ACSC (ASD, 2020 pp. 39–40). The ACSC was charged with threat analysis and information sharing to bolster not only government entities but also the private sector (ASD, 2020, p. 40). The culmination of this strategy was a public assertion of the hardening of the Australian cyber environment, enhanced by offensive cyber operations that would be carried out by various entities under the control of the government and with international partners.

For states such as China, this policy framework could be seen as a notable although imperfect development intended to affect their strategic decision-making and to deter them from conducting cyber attacks and cyberwarfare operations. In summary, consistent, clear and deliberate public messaging will remain an essential part of any cyber-deterrence approach.

2.7 Force Update in 2020

Given the potential for the deterioration of security settings in the Indo-Pacific region, the Ministry of Defence also issued the 2020 Force Structure Plan that promised even more

investment in cybersecurity to help shape Australia's strategic environment. This was a funding model with a total cost of AU$575 billion, of which AU$270 billion was to be invested in defence capabilities (Department of Defence, 2020, pp. 5, 53–56). Based on the government's strategic objectives,

> We will increase the Australian Defence Force's ability to influence and deny operations directed against our interests — ones below the threshold of traditional armed conflict, in what experts call the 'grey-zone'. This will involve boosting Defence's special operations, intelligence and offensive cyber capabilities, as well as its presence operations, capacity-building efforts, and engagement activities. (Morrison in Grattan, 2020)

The Force Update document discussed the 'Information and Cyber Domain' and deliberately emphasised military force design and the importance of cyberspace operations to the Australian Government in both force structure and posture. It again recognised the growing number of threats in the cyber domain alongside the ever greater reliance on digital technologies for many defence functions. Hence, future planned investments were aimed at protecting defence capabilities in cyberspace and enabling effective, resilient operations against adversary systems. In short, the document stated that ADF's deterrence capabilities should be strengthened, adding that 'capabilities and reach are expanding. Previous assumptions of enduring advantage and technological edge are no longer constants' (Grattan, 2020).

These funding and capability strategies extended investments in 'long-range' offensive cyber capabilities as well as operational cyberspace capabilities for deployed forces (Department of Defence, 2020, p. 27). What was also interesting was the scale of investment promised in this area, citing an AU$15 billion price tag over the next decade, which exceeded the promised investment of AU$1.7bn in the 2020 Cyber Security Strategy for the rest of the country (Department of Defence, 2020, p. 27). Part of these costs seemed to be premised on accepting that the private sector would continue to engage with Defence and would need assistance in cybersecurity measures or partial access to privileged systems.

As covered in more detail later in this thesis, a bulk of cyber funds would be appropriated by ASD and the program REDSPICE for a mammoth recruitment and skill uplift dedicated towards offensive cyber operations and the recognition that ASD would be the premier home of offensive cyber agency. For example, the 'Joint Cyber' program was created to incorporate offensive cyber capabilities alongside the ASD, and in part, provided extended strategic response options for the Australian Government (Department of Defence, 2020, p. 28). These

options implied Australian capabilities that could target the strategic assets of other nation-states, including actors such as China. The implication was that the government had multiple entities with attribution techniques, sophistication, coordination and resources that could hold Chinese assets at risk, which is a key pillar of Libicki's (2009) deterrence framework.

In relation to the overall 2020 Force Structure Plan (and the 2020 Defence Strategic Update), as Graham (2020) described, the ADF's 'basic force structure will not change significantly, the government has committed to acquiring long-range strike weapons and boosting offensive cyber capabilities with the explicit intention "to hold potential adversaries' forces and infrastructure at risk from a greater distance"'. Shoebridge (2020) commented that such active policy alterations, although not explicit, were, in part, based on a more assertive and provocative China, and that 'This change comes from US–China strategic competition, together with China's assertion of influence and use of coercive activities'.

Significantly, now prominent were 'grey-zone' activities designed to coerce in ways that aimed to stay below the threshold of military conflict—again, arguably similar to China's militarisation of the South China Sea. Graham (2020) commented about such deliberate assessments that 'although it (China) is singled out sparingly in the official text. References to countries that "pursue their strategic interests through a combination of coercive activities, including espionage, interference and economic levers" leave little room for ambiguity, however'. In short, while the government still appeared reluctant to formally identify China in these updates on defence capabilities, its assertions about rapidly changing regional contexts, the need for cyber reliance and the advantages of a security/military sector capable of extended deterrence had China dynamics clearly in mind. Overall, the ADF framework is designed to

> ensure our warfighting capabilities are survivable against adversary actions in cyberspace across all phases of war, including sub-threshold phases such as persistent contest and grey-zone operations and activities. It is, in essence, a risk management and continuous improvement framework, enabling the ADF to effectively manage our risk in cyberspace as we execute our mission. (Coyle, 2021)

In this sense, the 2020 strategic force update was notable for addressing the significant uplift in capabilities of the ADF cyberwarfare units, for tying them to the ASD and for asserting that they would be able to conduct offensive operations and not just function as a defensive entity (Department of Defence, 2020 pp. 27–28). Certainly, offensive cyber units with military backing are not without risk as regards escalation but are a principal deterrence-by-punishment

development for Australia. In this regard, Libicki (2009) reasoned that escalation is likely to occur if adversaries '(1) do not believe cyber-retaliation is merited, (2) face internal pressure to respond in an obvious or painful way, or (3) believe they will lose in a cyber tit-for-tat exchange but can counter in domains where they enjoy superiority' (p. 69).

In other words, in the context of this case study, the Chinese Government might be compelled to move towards escalation if a military entity (ADF) is seen as targeting a (Chinese) civilian asset because of internal domestic pressures and a political drive to see an opponent (Australia) punished for the action. Deploying military assets in a strategic deterrence framework is always underlined by risk–cost calculations and will always be multilayered. For Australia, the ASD would take on the lion's share of offensive operations and deterrence means in attempting to threaten a target into inaction. ASD credibility would also be a key factor in China's calculation of the defender's, that is Australia's, capability. This investment in defining penalty measures is best expressed in the ASD REDSPICE program.

2.8 REDSPICE

With the launch of REDSPICE, the Australian Government argued this program would enable ASD to keep pace with the fast-moving progression 'of cyber capabilities of potential adversaries. It provides new intelligence capabilities, new cyber defences to protect our most critical systems, and is a real increase in the potency of ASD's ability to strike back in cyberspace' (Withers, 2022). However, it is unknown what REDSPICE will involve specifically and what its activities might entail. Many questions remain about what offensive capabilities truly entail and what emerging technologies such as artificial intelligence (AI) or quantum computing will have on ASD operations. Despite this, the program is an immense step forward in the personnel levels of the ASD and is directly targeted at cyberspace.

In general terms, this initiative aimed to incorporate an increase in both analysts and automated systems to help to both identify and mitigate the growing number of threats and to deter continual cyber attacks with the threat of retaliation in a situation regarded as either peace or war. Such 'grey-zone' activities are coercive statecraft actions that are short of war. As Scott (2022) revealed, China's aggressive actions

> in cyberspace are part of a growing competition short of war in what is often … described as the grey zone. Australia's goal in this contest is not simply to win cyber battles – by having superior offensive capabilities – but to prevent cyberspace being transformed into a

> battlespace. Australia wants an open and secure global internet in which states behave according to accepted rules. So Canberra must use its growing offensive cyber capability strategically to avoid undermining this greater goal.

As an enhancement of national cyber capabilities, REDSPICE involves the investment of AU$9.9 billion in the ASD over 10 years up to 2030–2031 to deliver a Resilience, Effects, Defence, Space, Intelligence, Cyber, and Enablers (REDSPICE) package (see Fallon, 2022). The program aimed to double the ASD's size by adding 1,900 new jobs in the 10-year period and to bolster Australia's commitment to the Five Eyes and the AUKUS (AU: Australia; the United Kingdom: UK; and the United States: US) trilateral agreements (Parliament of Australia, 2022, p. 42). REDSPICE would also draw upon the abilities of the ADF, the AFP, Home Affairs and other agencies, and then hire 'new' talent to reach the government's desired hiring and capability numbers (see Dutton & Hastie, 2022).

Offensive cyber attacks can conceivably encompass anything from disruption of critical infrastructure to the manipulation of targeted data networks. As argued in Chapter 1, offensive cyber attacks as directed by a decision-maker are better described as a serious of effects orchestrated through the cyber domain (Seligman, 2022). Nevertheless, the aim of the program itself is to directly 'deal with changed strategic circumstances in the Indo-Pacific region, characterised by rapid military expansion, coercive behaviour and increasing cyber-attacks' (Greene & Dziedzic, 2022). It is with this in mind that the decision to expand the ASD 'acknowledges that cybersecurity is integral to the defence of Australia' (Fallon, 2022). Strategic circumstances in Australia's region, the Indo-Pacific, the rise of the cyber domain as an increasingly important warfare domain and the role the ASD will play all seemed to collide under the REDSPICE program.

This initiative, the related funding boost in both intelligence and cybersecurity capacity and the investment in foundational technologies build on work from past Australian Federal Governments across multiple iterations, which have been discussed throughout this chapter. Nonetheless, it is worth reinforcing that Australia began investing heavily in the capability of its cyberwarfare units from 2016 onwards, and its overlapping policy directions do appear to recognise that personnel themselves are often the primary conduits for cyberwar. This fact was emphasised by the targeted investment in the later 2022 budget and the revised cyber framework that moved beyond an entirely defensive or reactive approach (see Winkler, 2022).

Overall, in broad terms, REDSPICE can be seen as a high-end capacity investment in

> people, the application of modern and developing AI and Big Data techniques, and innovative intelligence and analysis practice. It also displays a refocusing of the way we as a country deal with offensive cyber operations and secure communications, drawing on the use of new technologies and bold and innovative thinking to do so. (Slay, 2022)

However, the secretive program is not without drawbacks and risks. In fact, the significant funding announcement involves some clever accounting—the proposed investment of AU$10 billion over 10 years is a raw truth, but in terms of new funding, the number is closer to AU$589 million a year (see Haskell-Dowland, 2022). Moreover, the funding boost towards ASD via REDSPICE was also critiqued in that the blueprint for addressing cybersecurity holistically is missing from the announcement (Tupas, 2022). For example, the private sector still required assistance to 'ensure that commercial and public enterprises can recover and get back to business quickly, beyond front door security measures' (Murray, as cited in Tupas, 2022). The argument that Australia focuses too much on cybersecurity at the 'front door', such as on patching applications password management, is thought-provoking. The program will have to contend with not only the private sector but also the sheer shortage of the relevant skills in the labour force of Australia in general. It will also have to contend with the reality that training any new software engineer takes years, not weeks, and certainly to the level that the ASD would need to deal with scaled cyber effects (Kremer, 2022).

Another possible future risk for REDSPICE, even presuming wide-ranging and sophisticated efforts to disguise the origin of an offensive cyber attack, is that the 'Australian Government could lose plausible deniability or be identified (including contextually) as the source and face embarrassment or retaliation' (Hanson & Uren, 2018, p. 8). Hence, at the very least, offensive cyber attacks would need to be highly tailored and purposeful to avoid causing indiscriminate and disproportionate damage. This again gives credence to the argument that decision-makers should request effects, with a clear scope of intended targets, and ask this of cyber-attack teams to determine whether it is possible to have such effects and within the desired scope (Seligman, 2023).

Overall, the public announcement for REDSPICE shows a drastic uptick and commitment in the operational capabilities of the ASD and the capacity of the Australian Government to respond in kind to cybersecurity incidents, although policy and legislative frameworks as well as wider strategic applications remain very embolic and/or secretive. Further, many questions

regarding cyber-power projection in grey-zone activities related to proportionality, risk management and avoidance of escalating to kinetic war remain unanswered. Nevertheless, as a starting point, the calibration of risk regarding China and the use of cyber force by the ASD need to be highly controlled and limited in order to raise the (real or perceived) costs, but only to the point where pursued Chinese cyber attacks are expected to be curtailed or abandoned.

2.9 Year 2022, New Government and the Deluge of Data Breaches

In May 2022, the Albanese Government was elected in the Australian federal election (Morresi, 2022). Despite the election campaign lacking a policy that offered significant differentiation or detail related to cybersecurity approaches, the new government entered with the expectation that some new bills would be introduced to create obligatory risk management programs and a mandatory ransomware notification scheme for businesses and government, which effectively borrowed and built upon an amendment proposed by the former Morrison Government (see Hendry, 2022). Nonetheless, this period of government was particularly critical in resource investments and efforts to improve the coordination and integration among government agencies and relevant stakeholders.

For instance, a notable action by Albanese was to appoint Clare O'Neil as Minister for Home Affairs and Minister for Cyber Security—the first time there was a portfolio for cybersecurity in the Australian Cabinet. Albanese also promised that the government would adopt a 'whole-of-society' cyber-deterrence approach and would support the ASD as the 'frontline' of defending against and deterring cyber attacks. O'Neil (2022) reinforced that a key part of investment in the ASD was in REDSPICE, which was noted as further hardening of Australia's cyber defences and further strengthening its cyber resilience, which was regarded complementary to both passive and active cyber operations.

Yet, such work to build Australia's cyber defences, in particular, deterrence by denial, and to respond to cyberthreats was immediately tested because of multiple significant data breaches in the second half of 2022. In particular, the cyber attacks on Optus and private health insurer Medibank dominated cybersecurity news and awareness campaigns in Australia. These attacks not only led to calls to boost Australia's cybersecurity as a national priority but also led to O'Neil implying that certain private companies been lax in cyber hygiene and that Australia must prepare for a dystopian future (cited in Hurst, 2023). She also labelled unnamed state-sponsored attackers as 'the apex predators' and stated Australia and other allied countries

would ‘call out and attribute these threats where it is in our national interest to do so’ (Hurst, 2023). Further, O’Neil flagged new laws in the cybersecurity space and promised to re-prioritise funding. She said:

> This is a huge wake-up call for the country. And certainly gives the government a really clear mandate to do some things that frankly, probably should have been done five years ago, but I think are still very crucially important. (Bucci, 2022)

In addition, in November 2020 the Albanese Government announced a new taskforce, combining the expertise of the AFP and the ASD, to ‘hack the hackers’ (Lapham, 2022). O’Neil added that one of the main aims of the new Labor Government was to disrupt and discourage hacking operations and not allow Australia to be a ‘soft’ target while acknowledging that cyber attacks were relentless and remained a core national security risk (Lapham, 2022).

The Optus data breach was the largest in Australian history in terms of the number of victims, with roughly 11 million Australians either directly or indirectly affected by the colossal cyber incident (Toulas, 2022). The breach was facilitated by the attacker using an unsecured application programming interface (API) to steal data as opposed to breaching the company’s internal systems (Toulas, 2022).

An API is effectively a tool that internet users use to communicate rather than Optus’ own servers directly. The issue was that this API had no authentication required to access it and when opened up, it provided a trove of data for the attacker (Kirk, 2022). The threat summary of this event is that the attack was essentially one of ‘opportunity theft’ rather than a sustained sophisticated operation, despite the initial attempts by the Optus chief executive officer to frame the breach in those terms (Bonyhady & Knott, 2022). The attacker/s had initially attempted to extort Optus by threatening to openly publish certain sets of private data to prove their legitimacy but later claimed to have deleted all the data instead (Wilson, 2022). In blunt terms, it is illegal to break into a car and steal someone’s private property; however, an insurance company will still criticise the individual for leaving their valuables in plain sight.

The political flow-on effects were immediate with O’Neil citing the inability of prior legislation to impose mandatory cybersecurity requirements for telecommunications companies within Australia’s deterrence cybersecurity architecture, in part because of the prevailing attitude among these companies of ‘Don’t worry about us – we’re really good at cybersecurity. We’ll do it without being regulated’ (L Evans, 2022). The result can be seen as a ‘trust degradation’

between the Australian Federal Government and much of the telecommunications industry. Further, it triggered a review of cybersecurity practices across industry. As stated, the Optus chief executive officer was adamant that the attack was 'sophisticated', until O'Neil completely denied those inexact statements and categorised the attack instead as 'simple' (see Bronyhady & Knott, 2022). In February 2023, the government announced the establishment of a Coordinator for Cyber Security, in the Department of Home Affairs, to assist in continuing to build 'whole-of-nation' cyber resilience and ensuring a centrally coordinated approach to deliver newly mandated cybersecurity responsibilities (O'Neil, 2023).

For example, modern mandated practices include enforcing the use of protective domain name system services in order to prevent malware and other infections from malicious websites (see Hendry, 2022). There had also been calls from the Department of Finance (2022) to seek proposals from suitably experienced entities to provide web application protection services for a 'whole-of-government' arrangement for not only web apps but also APIs. Thus, the Australian Federal Government appeared to be moving from accepting at face value the claims that industry and government had implemented 'best practice' to mandating them—and proposing penalties for repeated or serious data breaches (O'Neil, 2023).

Similarly, the Medibank breach affected 3.9 million customers with an extraordinary level of data breach that exposed even details of medical procedures (Taylor, 2022). Unlike in the Optus data breach due to the API, Medibank's main issues were not caused by valuables left on the car seat. Rather, the initial analysis revealed that Medibank had been targeted by a more 'sophisticated' actor that had pilfered credentials and then used them to leverage greater access, although the attacks were still relatively cheap and easy (Mason, 2022).

Moreover, the attacker/s appeared, or were at least linked to, the Russian Government: the REvil Ransomware group (Mason, 2022). Regardless, it is possible the attack was also a crime of opportunity as the exploited account was that of a support desk worker that did not have two-factor authentication enabled (Morton, 2022). Thus, the attack was able to lurk for weeks without detection and exfiltrated troves of data (Morton, 2022). In 2020, a similar hacking incident had occurred when attackers—linked to China allegedly—stole more than 300 gigabytes of data, including technical information, from an Australian defence contractor, (Hurst, 2020). Thus, in 2023 the government banned federal employees from installing the Chinese social media app TikTok on their work devices.

The Optus and Medibank breaches exposed many realities of ‘whole-of-government’ efforts. First and foremost, it became clear was that many of the larger Australian enterprises, especially in the telecommunications sector, had insufficient capability or willingness to adequately protect sensitive data against relativity low-level attacks despite their repeated reassurances (O’Neil, as cited in Palmada, 2022). O’Neil (2022) claimed, ‘the truth is, we are unnecessarily vulnerable. We did not do the work nationally over the last decade to help us prepare for this challenge’. The Minister very bluntly stated that the data breaches were not a new phenomenon and Australia needed to have meaningful deterrents, which would require greater collaboration between government and industry partners in terms of data security. Other cybersecurity experts even warned that Australia remains the ‘weakest link’ in AUKUS and will need to tighten its cybersecurity credentials: ‘We need to treat the information … shared by the Americans and the British with the same degree (of caution) that they would. These are among their most strategic secrets’ (Croft, 2023a). Further, ASIO also identified AUKUS-related initiatives as an imminent target for hostile cyber actors (Van der Schyff, 2023).

Nonetheless, the overall policy response to the threat landscape and to ascertaining ways to conduct strong cyber deterrence has been multifaceted under Albanese. This has included investments in network resilience and the incorporation of the signalling of the formation of an offensive cyber-operations group with the intention to ‘hack back the hackers’—that is, a threat to launch operations to uncover and potentially cause damage to cyber attackers and their systems and networks (Pearson, 2022). The stated scope of this group is seemingly unlimited and it would ‘scour the world, hunt down the criminal syndicates and gangs who are targeting Australia in cyber-attacks, and disrupt their efforts’ (O’Neil, quoted in Speers D, 2022). This response again signals potential costs to an adversary and arguably showcases Australia’s capability.

Notably, as part of a signalling framework to help deter aggression in cyberspace, it was also announced that the offensive cyber-operations group will ‘not be a model of policing, where we wait for a crime to be committed … we are offensively going to find these people and hunt them down and debilitate them before they can attack our country’ (O’Neil, quoted in Speers D, 2022). This distinction is an important policy growth from prior cyber defences that were focused on ‘defending the front door’ and built from the punishment task set out from the Turnbull Government, which emphasised the offensive nature of the ASD in the 2016 (Murray, as cited in Tupas, 2022). In short, the Australian Government appeared to embrace the notion

that open signalling remained an essential component for coercive diplomacy and cyber deterrence.

Again, there could be some drawbacks to any offensive 'hack back' operations. One commonplace concern is that if the country takes a disproportionate offensive stance, it could 'put a big red cross on Australia's back' (Alazab, 2022). For instance, deterrence operations in the cyber domain require attribution of attackers, and hence, any inaccurate or disproportionate response could lead to unhelpful escalation (Alazab, 2022). As Libicki (2009) noted, policymakers should ensure that they recognise and apprehend the parameters of any attack and each party remains responsible for managing escalation should operational tensions develop. Consequently, what remain difficult challenges for offensive operations are the ability to precisely attribute and select targets and the idea to 'disrupt, deny, degrade or destroy' adversely capabilities in a policy backdrop of how escalation options and risks should be treated. Hence, 'Those who would manage escalation by exercising self-restraint and persuading adversaries to do likewise should start with a sense of what the other hopes to get from unilateral escalation – that is, crossing some hitherto uncrossed red line' (Libicki, 2021, p. 74).

As aforementioned, in terms of private–public partnerships in Australia, the government also unveiled through new legislation punishments under the adapted SOCI Act for private entities. It increased the maximum penalties from the original AU$2.2 million for serious breaches to either AU$50 million or 30% of a company's adjusted turnover in the relevant period (Dreyfus, 2022). Importantly, the greater of these punishments will be applicable, which has resulted in a huge increase in the penalty payable. Indeed, the penalty could have been in the hundreds of millions for some of the recent breaches that occurred before this legislative change became applicable (A Brown, 2022). Further, any cyber incidents must be reported within 12 or 72 hours of becoming aware, depending on whether a material disruption to essential goods or services has occurred.

The SOCI act also provided the Australian Information Commissioner greater powers to resolve data breaches, strengthened the Notifiable Data Breaches scheme to ensure the Commissioner had comprehensive knowledge of information compromised and equipped the Commissioner with greater information-sharing powers (Dreyfus, 2022). Alongside these punishments was the addition of cybercrime to the Attorney-General's ambit, indicating how large-scale cyber attacks will be divided and distinguished in deterrence responses: O'Neil and

the ASD would focus on ‘hunt and deter’, while the Attorney-General’s office would tackle the police response and legal repercussions (Massola, 2022). Overall, the legislation placed the onus on private and public institutions to ensure that they not only had the capacity to detect a cyber attack but also would act quickly to resolve it.

It does remains to be seen whether this new period of cyber deterrence and digital transparency will produce the desired behavioural outcomes—but certainly, many of the security issues present in the Optus and Medibank breaches were considered the outcomes of highly negligent and too casual reporting requirements (as opposed to obligations; Swinson, & Bowe, 2022). Therefore, the new penalties might encourage executives in major companies to ‘sweat a bit’ on cybersecurity and to be more effective in dealing with digital risks, including through employee awareness and training and adopting a written risk management program. Government assistance would also be available to Australian industry as a potential last resort in cyber incidents.

Overall, the 2022 hacking events spurred an avalanche of policy action. The Albanese Government appeared to accept an increasing level of federal responsibility for the sanctity of data stored in Australia while admonishing the private sector for its failure to do so—the importance of data and cybersecurity was clearly evident, particularly for those whose systems had been declared as ‘of national significance’ (O’Neil, quoted in L Evans, 2022). REDSPICE would also continue to be boosted in efforts to enhance and transform Australia’s ability to respond to the rapidly developing cyber landscape – in part, by impressing adversaries such as China with the likely effects of offensive cyber attacks by Australia.

2.10 Conclusion

Accordingly, what has been the historic development of cybersecurity in Australia, and what may the future hold? What are the technical abilities at the disposal of the Australian Government? What are its key objectives in the cyber domain? What has the rate of growth been for the Australian Government towards establishing a strong cybersecurity infrastructure? All these questions will require engagement and alliances with industry and stakeholders as consecutive Australian Governments have aimed to lift cybersecurity protections across the country. Certainly, given the changes in 2002, the private sector will no longer be able to pitch a ‘she’ll be right, mate’ approach. Moreover, the government moved into an active as well as

passive deterrence space and publicly acknowledged Australia's cyber-offensive capability with REDSPICE to serve as a warning.

Yet, one catch is that Australia itself might not know how resilient or vulnerable its own systems are these until actually tested. Nevertheless, all the above questions are critical to deterrence discussions as any state that falls behind technologically and strategically in the cyber domain will, at the very least, be considered vulnerable to perceptions of weakness by other states in any calculation in their own risks from action and aggression. The above policy lifeline displays, in part, how cyber capabilities and logic in Australia have steadily evolved to increasingly offer enhanced cyber resilience as well as a defensive and offensive coordination and related opportunities for policymakers. This has included elevating the National Cyber Security Coordinator role as part of a Cabinet process in 2023. Indeed, the appointment of O'Neil as a dedicated Minister for Cyber Security in itself should be considered a powerful signal by the Australian Government of a policy commitment towards advancing cyber deterrence.

Concurrently, the creation of the Essential Eight Maturity Model has been a significant step in at least defining security standards for Australian entities to follow, and mandating government entities to aspire to (Australian Cyber Security Centre, 2023). The ACSC asserted that while no one set of mitigation strategies are guaranteed to protect against all cyber threats, businesses are recommended to implement eight essential cyber security strategies, which is intended to harden as much of Australian cyberspace as possible (Australian Cyber Security Centre, 2023). From a deterrence perspective, this model would be useful not only because it ensures deterrence-by-denial capacity, but also because functioning networks from which government agencies can launch cyber attacks are necessary for deterrence-by-punishment methods.

Therefore, for a digitised society such as Australia, operational and capacity gaps in cybersecurity and cyberwarfare will not only cast doubt on the value of cyber deterrence but also expose its citizens to future destabilisation and instability. In short, to remain a credible actor in the cyber domain, Australia will need to present itself as having clear, deliberate policy goals and the capacity and will to successfully execute them within a whole range of possible deterrence strategies. Central to this goal is arguably the ASD in its new-found offensive purpose and its ability to defend Australia from cyberthreats and to work with government and industry to detect, disrupt and respond to threats—such as to even strike back when necessary. To reiterate, for avoiding escalation, such offence tools should also always remain proportional

and ‘tit for tat’. Significantly, there are many unanswered questions about REDSPICE. Meanwhile, private industry clearly must perform better in protecting customer data and implementing deterrence-by-denial best practice. Hence, one clear pattern that emerges from the above cyber-policy time line is that Australia’s cyber-deterrence strategy has quickly become a deliberate ‘whole-of-nation’ endeavour, predominately in deterrence by denial while the ASD will lead the charge in deterrence by punishment.

Significantly, The Cyber Defense Index conducted via the MIT Technology Review assesses the world’s 20 largest economies, and then ranks all these countries based on preparation against, and response and recovery from, cybersecurity threats (O’Brien, 2023). In 2023, these 20 countries were evaluated across four core standards—critical infrastructure, cybersecurity resources, organisational capacity and policy commitment—and Australia ranked first in three of the four pillars to obtain a top aggregate score of 7.83 (MIT Technology Review, 2023). This ranking reflects, at least in part, consecutive commitments by the Federal Government to provide a centrally coordinated approach, to build cyber resilience, to use regulations to safeguard personal data more effectively and to adapt cybersecurity laws (especially in 2022) in Australia, as discussed in this chapter. Hence, in general terms, Australia appears to have steadily and incrementally built an adaptive cyber-deterrence environment, including for securing critical infrastructure and by creating the IWD. However, these policy approaches also all highlight the permanence of cyberthreats, including those from China.

Accordingly, in terms of the key research question—‘Is cyber deterrence by punishment possible?’—Australia has invested heavily in capacity, especially since 2016, by adding a deliberate, although initially secretive, deterrence-by-punishment mechanism. IN addition, since government agencies and critical entities in the private sector use and store data on the vast majority of Australian citizens, Australia’s deterrence strategy has been built on the public-private partnership model. As a start, with mandatory reporting and ACSC actively supporting information sharing and related engagement with the private sector, current (and future) governments can conceivably draw a much more accurate picture of the Australian network, its vulnerabilities and where and when intrusions do occur. This approach remains important for not only detecting potential attacks but also ensuring attribution, as discussed in more detail in Chapter 4—which the ASD is now authorised to perform. In other words, sharing threat information and ensuring increased cooperation has and will boost the effectiveness of

cybersecurity and advance cyber deterrence across the threat landscape, including in dealing with China.

Certainly, given the major hacking incidents in 2022, the private sector's reputation has undergone some significant damage (see Palmada, 2022). This reputational damage to the telecommunications industry—which had initially asserted that it did not need government oversight because of its own upskilling and capabilities—was especially humbling for telecommunications entities in Australia. Nevertheless, these events also provided an opportunity for the Australian Federal Government to step in and to require that specific critical infrastructure assets must report certain types of cybersecurity incidents. Furthermore, the notion itself of a 'critical infrastructure asset' also covered a much broader range than covered previously (and the government can then further conceivably authorise the ASD to take direct retaliatory action where necessary).

Significantly, a short reporting timeframe may translate into an early ASD investigation that could be rushed and disproportionate may result in erroneous or missing attribution details. However, it can be argued that the benefits might outweigh the risks. As one security expert commented:

> I mean, in some cases, it can take months and even years to really truly find out what is actually going on. And so, yeah, ultimately, the conclusions and the information and the evidence you identify may not be entirely or certainly won't be the full story and may not be entirely accurate. But that being said, what is important is sharing that information with trusted parties, which actually allows us the opportunity to be able to share what we know to other organisations that may also be part of that campaign. (Croft, 2023)

Accordingly, despite a slow start in the 21st century, marked by a poor recognition of cyber hygiene and a flimsy 'whole-of-society' mindset, the Australian Government has progressively emphasised cyber defence and later offensive cyber operations towards creating a capable, effective cyber force with a robust, modern capacity and intent. Thus, while actors such as China will continue to search for opportunity (see the next chapter), there has been a steady, robust, although sometimes ad hoc and reactionary, movement towards deterrence safeguards and a much stronger cybersecurity platform of policy development. This includes the investment of increased time and money into cybersecurity, legislative actions to support data sharing within Australia and the use of signalling to deter potential attackers. Nevertheless, examining what the Chinese are capable of is, in turn, essential to examining how effective

Australia can be at responding to, and deterring, cyber attacks from China, which is examined in the next chapter.

Chapter 3: China’s Cyber Strategy

3.1 Introduction

Any Australian security approach to deterrence, risk management and the use of cyber forces to strike strategic targets will need to comprise a sophisticated understanding of the values, credibility, cyber capacity and related policy agendas, of potential rival states such as China. It is crucial for Australian deterrence considerations that there is an understanding of Chinese policy developments, which would then inform when cyber attacks have occurred, where they have been launched from, and how these attacks may occur. Critically, as explored in this chapter, China’s denial and deception activities in the cyber realm include concealing via secretive bodies such as Unit 61486, which is a People's Liberation Army (PLA) unit dedicated to cyber attacks. Understanding Chinese practices related to forming and subsequently dissolving these units, which are often listed as APTs, will be critical for Australian decision-makers formulating deterrence-by-punishment practices that can be effective and capable, and not just Australia’s own capabilities as explained in the previous chapter.

Significantly, various Chinese leaders themselves do not necessarily hold definitive views on conducting cyber operations, and much of the investment in its cyber capabilities may be attributable to China’s overall desire to ‘catch up and surpass’ the technological capacity of competing states and boost its own digital development. This mindset is also represented in how cyberwarfare tactics are changing, such as accusations against China about cyber-enabled espionage and its ‘rob, replicate and replace’ agenda (see Gewirtz, 2019). Such cyber attacks that aim to steal and copy intellectual property can have direct or cascading risks for Australia. As already stated, recent studies have found that China is responsible for more than two-thirds of state-sponsored cyber attacks worldwide (Galloway, 2021). These attacks have included malicious cyber activities against Australian telecommunications, as explored in the previous chapter. This activity is interesting when considered alongside MIT’s Cyber Defense Index, which placed China in the bottom 10 of the top 20 global cyber powers, citing a ‘poorly regarded infrastructure resilience and difficult polity environment’ (MIT Technology Review, 2023, p. 7). Is China all aggression and lacking on the defence front, and can Australia exploit this aspect to enhance its deterrence capabilities?

This chapter address the context of China’s policy, deployment logic and move from a developing cyber entity to a very sophisticated actor in cyberspace that has the ability to

increasingly exploit vulnerabilities on servers and networks (Volz, 2023). China's 2015 Ministry of National Defense paper entitled 'China's Military Strategy' also described the primary objectives of its cyber capabilities to include 'cyberspace situation awareness, cyber-defense, support for the country's endeavours in cyberspace, and participation in international cyber cooperation' (State Council Information Office, 2015). The strategy outlined these objectives with the aims of 'stemming major cyber crises, ensuring national network and information security, and maintaining national security and social stability' (State Council Information Office, 2015).

Thus, the investigation in this chapter will be conducted by analysing both official policy documents and secondary sources that consider and discuss (and often translate) the building and development of China's cyber focus and strategy. This review of the literature is intended, in part, to clarify what is otherwise often an opaque picture about Chinese cyberwarfare intent and capabilities, both technical and political, in order to better assess the likelihood that an Australian deterrence architecture utilising Libicki's (2009) framework could mitigate cyber attacks from China against Australia and also avoid unintentional escalation.

Further, in general terms, the Australia–China rivalry occurs within the scope of a convergence of modern-day electronic and information warfare. In this regard, Libicki (2017) summarised that destabilisation and particularly subversion are the starting points for multiple elements of information warfare:

> The point of subversion is to usurp the normal state in which systems do only what their owners want. Instead, they do things hackers want. In some cases hackers can get systems to react to inputs in unexpected ways, and in other cases such systems can execute an arbitrary set of commands provided by hackers. Once hackers compromise a system they have many options. (p. 51)

Significantly, China is very active in creating subversion in the cyber realm, and its building and display of its capabilities poses a serious challenge for Australian policymakers. China's ambiguity and denial may be exploited to curb and reduce the risk of reprisals via, for instance, the ASD. China has repeatedly and consistently rejected accusations that it is to blame for cyber attacks. For example, when accused by the US of hacking Microsoft Exchange email systems in 2021, China's Foreign Ministry spokesperson Zhao Lijian stated that the accusations were 'purely a smear and suppression with political motives' (*China Rejects Accusations Of Cyber Attacks,* 2021). Similarly, in 2023, China's authorities denied any form of state-sponsored

hacking, and instead, claimed that China itself is a frequent target of cyber attacks. The PLA even called the US 'the empire of hacking' while arguing that that identifying the source of cyber attacks was 'complex' and warning against 'groundless speculations and allegations' (Potkin & Geddie, 2023).

Hence, assessing the parameters of a cyberwarfare will require investigation of whether China is aware of such cyber attacks and a political context in which it claims that such accusations are always baseless. It has demanded that Australia stops 'throwing mud' at China on cybersecurity issues and has also made open-ended and indistinct claims that it 'will take necessary measures to firmly safeguard China's cybersecurity and interests' ('China Hits Back at "Fabricated" US Hacking Allegations', 2023). Conversely, there has been extensive dialogue on China's wrongdoing and its aggressive cyber operations relating to espionage, which have gone from speculative discussions to the more deliberate and public assessments that China regularly develops and deploys advanced, zero-day exploit-level cyber attacks daily (see Gen. Alexander in Rogin, 2012; former FBI Director Comey in Osborne, 2014; O'Neill, 2022; Plis, 2021).

In this sense, China's own cyber-governance regime is best understood as a complex mix of interconnecting strategies, positions and sometimes vague or open-ended standards. However, its formal cyber policy itself has been traditionally evolved by a wide range of defence, law enforcement and related regulatory agencies designed to achieve four central goals:

> First, to maintain tight control over the flow of information to ensure domestic stability. Second, China wants to reduce security vulnerabilities in critical networks and defend the country against a range of cyber operations, including espionage as well as disruptive and destructive attacks. Third, Chinese leaders want to ensure technological autonomy, diminish reliance on foreign suppliers, and help Chinese companies dominate markets in emerging technologies. Finally, Beijing looks to expand its influence over cyberspace and limit the room for manoeuvre for the United States and its partners. (Segal, 2020, p. 1)

Further, various official papers published in *The Science of Military Strategy* (SMS) focus on China's national security strategy. The SMS is one of the main doctrinal military publications of the PLA. As stated in 2015, with cybersecurity having a much greater emphasis in military security outlooks:

> China will expedite the development of a cyber-force, and enhance its capabilities of cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation, so as to stem major cyber crises, ensure national network and information security, and maintain national security and social stability (State Council Information Office, 2015).

Last, in keeping with Libicki's (2009) framework, this chapter will also incorporate a review of Chinese cyberwarfare developments and investigate the capacity of the Chinese Communist Party (CCP) to conduct strategic-level cyberwarfare. As stated, this will be necessary in then accurately assessing whether Australia can legitimately provide the means—technical, political or willpower-related—to deter China from conducting damaging cyber operations. Cyberspace presents incredibly unique challenges that do not automatically present in more conventional warfare scenarios, including the role of ambiguity and proxy warfare (see Chabrow, 2009).

3.2 Chinese Actions as a Cyberthreat

In 2022, then Defence Minister Peter Dutton claimed that China's cyberwarfare capabilities had the capacity to mount 'an unprecedented digital onslaught' with its online weaponry seen as growing in parallel with its military build-up (Tillett, 2022). Dutton also added that China used cyber operations to pursue its national goals by engaging with rivals below the threshold of war, which is again an issue that might complicate attribution and create a strong character of ambiguity.

Similarly, former senator James Paterson, who was head of the Parliamentary Committee on Intelligence and Security in 2021, stated that economic coercion 'has not worked as well against us as (China) may have hoped, but cyber-attacks emanating from China against government entities and critical infrastructure providers is absolutely relentless' (Burke, 2021). Other countries such as the US have also raised similar concerns about China's demonstrated willingness to use cyber attacks as a tool of coercion. In 2019, Lieutenant General Robert P. Ashley argued in a Defense Intelligence Agency's analysis that

> Chinese leaders characterize China's long-term military modernization program as essential to achieving great power status. Indeed, China is building a robust, lethal force with capabilities spanning the air, maritime, space and information domains which will enable China to impose its will in the region. As it continues to grow in strength and confidence, our

> nation's leaders will face a China insistent on having a greater voice in global interactions, which at times may be antithetical to U.S. interests (Defense Intelligence Agency, 2019).

Thus, Australia has had to engage in a tricky balancing act in efforts to manage a more aggressive China and its catalogue of threat actors and cyber tactics. The China–Australia diplomatic relationship itself has been under increasing strain in recent years, often spilling out into public displays of acrimony, intimidation and breakdown (see Hunter et al., 2023). Indeed, the rhetoric of some Australian political leaders and media commentators has even emphasised 'that Australia faces an existential threat to its security and prosperity from a rising and more assertive China' (Collinson, 2023). Collinson (2023) also argued that this mentality of an existential threat is often compounded by how Australia approaches China from a security and risk perspective, although at the very least, resolving uncertainties should be a priority to reduce the potential for misperception and to dampen spirals of mistrust. Moreover, in addressing the nature of risks, the character of war is transforming with respect to cyberspace operations with China's approach to defence industrialisation emphasising CCP sovereignty in cyberspace and its technological rise (see Austin, 2014, p. 42).

Indeed, a cornerstone of China's position on cyber governance is the concept of cyber sovereignty. This concept first appeared prominently in China's 2010 white paper that outlined its approach to cyberspace. From this angle, China's approach is often interpreted as provoking competition and exporting its authoritarianism, particularly through its Digital Silk Road via the Belt and Road Initiative:

> China has been exporting its digital infrastructure, along with its digital governance model, to BRI [Belt and Road Initiative] member countries … In the realm of cyberspace, unlike physical resources such as oil or critical minerals, data, as a virtual entity, doesn't conform to traditional jurisdictional boundaries. This reality has complicated the issues of data sovereignty and data governance, particularly with the rise of advanced digital technologies, such as AI, cloud-based computing and data analytics (Zhang, 2023).

In addition, given the lines of tension being drawn around interpretations of data sovereignty, Australia and China have been at odds about the shape of the 'world order' in cyberspace, which has incorporated debate points around issues such as information exchange, data sharing, cyber governance, individual privacy and data security (see Packham, 2019). Meanwhile, Chinese spying activities and attacks have continued, including by government and military actors, contractors, patriotic hackers and criminal elements (Gady, 2016). Hence, in broad

terms, such aligned interests among different and diverse groups ‘may drive activity that blurs the lines between direct government sponsorship and independent action’ (Gady, 2016). Therefore, a more refined approach to cyber operations by China has complicated approaches to malicious activities in cyberspace owing to its non-monolithic character.

In sum, various reported cyber-attack instances (Borys, 2019; Farley, 2019) against Australia can be seen as representing China’s willingness to conduct espionage operations and intrusions via cyber means into sensitive Australian digital architecture, which affects thousands of computers and networks. Therefore, such large-scale, sustained online attacks have placed successive Australian Governments in the difficult position of deciding whether to outright attribute this activity to China or to employ more diplomatic or even aggressive countermeasures (see Chapter 5).

As also explored in Chapter 4, ambiguity, diplomatic denial and the level of sophistication of many of the Ministry of State Security (MSS) attacks has made attribution challenging, such as in attempts in 2020 to steal information linked to Australia’s COVID-19 response (see Welch, Hui, & Dziedzic, 2020). Moreover, such attacks and cyber intrusions have continued to exploit known vulnerabilities, and Australian policymakers and the ASD have repeatedly attempted to identify the tactics, techniques and procedures of adversaries, even for relativity unsophisticated DDoS attacks, given the large scope of non-monolithic origin sources (Uchill, 2019).

For example, in essence, many target victim entities in Australia have not enforced security programs that raise the bar on the attacks that will actually work against them, which enables actors to still utilise low-level cyber attacks that are relatively easy, replicable and duplicable. As Welch et al. (2020) argued, since the number of entities that can deploy these ‘easy’ methods is wide and diverse, this allows obfuscation and culpable deniability. That is, a suspected attacker can challenge, ‘How can you certifiably prove it is us if it is an attack that anyone can and does do?’ (also see Buchanan, 2017). This has led to the security and risk management phrase, ‘If everything is sophisticated, nothing is’ (Uchill, 2019).

Even in the backdrop of such ambiguity, Australia and others have consistently accused China of directly or indirectly spying on energy and internet companies and other targets. One noteworthy incident was in June 2021, when the US was joined by NATO, the European Union, Australia, the UK, Canada, Japan and New Zealand in condemning cyber spying and with the

US Department of Justice formally charging four Chinese nationals: three security officials and one contract hacker. US President Joe Biden added that 'my understanding is that the Chinese government, not unlike the Russian government, is not doing this themselves, but are protecting those who are doing it. And maybe even accommodating them being able to do it' (Holland & Chiacu, 2021).

In another instance, in June 2023, Australia was among four countries whose government officials were targeted by suspected China-based hackers, who attempted to install malicious software and steal information, after a Group of Seven meeting in Japan (Mason, 2023). In short, China can be seen as actively engaging with Australia, as well as in the region, in the cyber-espionage space and in related campaigns across a spectrum of arenas of ambiguous engagement with increased scale and severity. Such actions in the cyber domain have been exacerbating diplomatic tensions and economic disputes, destabilising a fragile relationship between Australia and one of its most significant partners, China (Andrews & Dutton, 2021).

For its part, China appears increasingly willing to test boundaries and to flex diplomatic, economic and political muscles to attain its goals in shaping its environment, included in the cyber domain. In January 2013, the PLA's Lieutenant General Qi Jianguo stated:

> Cybersecurity concerns national sovereignty as well as the security of economic and social operations, and it concerns the quality of human existence. The West's so-called 'internet freedom' actually is a type of cyber-hegemony. In the information era, seizing and maintaining superiority in cyberspace is more important than seizing command of sea and command of the air were in World War II. (Inkster, 2013b, p. 10)

Such comments by Chinese security holders are certainly useful for framing Chinese perspectives on cyberspace and the ongoing CCP perception that owing to Western dominance over the internet—a perception that is based on the perceived Western control of the internet's founding infrastructure and the fact that many corporate IT firms are located in Western countries such as the US—the CCP is under threat by a cyberspace hegemon with unique command of that domain. Therefore, from a Chinese perspective, it has had to also increase investment in cyber (and space) capabilities for defensive purposes (Gewirtz, 2019).

Nonetheless, constructing a picture of the Chinese cyber landscape and of the Chinese Government's views of that domain and related security dilemmas will be informative in assessing how Australia's deterrence policy could be shaped and adapted. Again, this is

particularly important as cyber-deterrence campaigns need to be tailored to deal with specific adversaries—as stated in earlier chapters, sweeping deterrence ideas that are too vague and not specific to the intent and capacities of an adversary will be much less efficient and credible than targeted responses in the cyber domain.

In terms of intent, China seeks to advance its national security through the control of cyber means. Part of this reasoning is because central information organisations and outlets in China are often focused on dealing with domestic control/order, social security and 'ideological heterodoxy' (Inkster, 2013). In short, cyberspace is not only seen as not supporting and advancing the operation and interests of the state apparatus internationally, 'but also becomes a dependence on the lives of enterprises, the public, and even individuals' (China Aerospace Studies Institute, 2020, p. 149).

For much of the 20th century and into the 21st, China has deployed IT in service of a one-party political apparatus geared towards ensuring domestic security, enforcing strict party doctrines and enshrining the CCP as the prevailing political force in the country (see White, 2013). Subsequently, China has curtailed the free flow of information in efforts to establish robust cyber capabilities for exerting domestic control and dominance. As Feakin (2013) revealed:

> Traditionally, the key targets for such attacks have been Chinese democracy activists, Tibetans, the Uighur community, Falun Gong practitioners and supporters of Taiwanese independence, as well as others who may paint a negative picture of China both at home and abroad. Essentially, the cyber-domain has meant that political dissidents of any persuasion, who in the past were too far away to be reached, can now be tracked clandestinely.

Events as early as in 1990–1991 represented a significant and expanded turning point for China in the development of a more cyber-oriented mindset and a related international cyber posture. For example, the Operation Desert Storm combat in 1990 in Iraq highlighted the speed of US-led coalition forces on using the latest technology, in what was eventually known as a revolution in military affairs (RMA; see Sloan, 2002). Not only were 'smart' weapons observed to be highly successful and valuable, but also robust command, control, communications, computers intelligence, surveillance and reconnaissance (C4ISR) capabilities were assessed to be indispensable on the battlefield (Yu, 2022). One apparent lesson was that emerging military technologies would fundamentally change warfare.

The recognition of these evolving technological capabilities, connected to organisational and strategic adjustments, and the 'new' relationship between military technology and warfighting compelled the CCP to invest heavily in concepts of cyberspace and cyber power and to make large capital advancements in the world of computers, advanced weaponry and cyber-enabled technologies (Dahm, 2021). Furthermore, in preparing for the new RMA tasks, cyber espionage was fit for national security purposes, such as being able to pilfer sensitive military documents or penetrate competitors' computer and communication systems to steal new technological blueprints with security implications. Therefore, this strategy to exploit cyberspace was both about the immediate control of information and data and the future 'preparation for military struggle' (Bhattacharjee, 2023). Thus, for China, cyberspace is the battlefield of operations for cyber conflicts.

3.3 Unrestricted Warfare in 1999

In 1999, two Chinese colonels, Qiao Liang and Wang Xiangsui (1999), published a text entitled *Unrestricted Warfare* (Liang & Xiangsui, 1999). The text was instructive as an endorsement of what can be referred to as asymmetric warfare in the realm of international affairs: an effort for rising powers such as China to bridge the capacity divide between themselves and the US (Bunker, 2000). *Unrestricted Warfare* is a fascinating study that provided an unofficial insight into the mindset of officers in the Chinese military, one of whom eventually rose through the ranks to Major General in the PLA (Weiss, 2023). In dealing with forms of militarised conflict, the book is instructive of how emerging officers in the PLA were conceiving the dynamics of future interstate contest, including what would later be widely labelled the 'grey zone', which is an area between peace and war.

In the text, Qiao and Wang suggested how to best deal with the US when there is a clear disparity in outright military power and technology projection between the US and China. The authors noted that there is no nation on earth at the time of writing that could directly match the US in the physical field of battle. They made this assertion after observing the crushing defeat of the Iraqi Army in Operation Desert Storm as well as US military doctrine, and they mooted allied support in potential conflict scenarios such as across the Taiwan Strait. It is worth noting that despite the focus, the text is also instructive for an Australian-based deterrence thinking, given that *Unrestricted Warfare* offered itself as a manual for China (as well as other powers) and claimed there was 'no longer a distinction between what is or is not the battlefield' (Qiao & Wang, 1999, p. 207). The authors added that 'boundaries between soldiers and non-

soldiers have now been broken down, and the chasm between warfare and non-warfare nearly filled up' (Qiao & Wang, 1999, p. 223) – hence 'unrestricted' in going beyond the sphere of the military, and combining civilian entities in the warfare effort.

However, the book itself has never been confirmed as an official policy document although it is still popular and widely read, and even former President Jiang Zemin and the then Minister of Defence Chi Haotian have purchased it (see Bunker, 2000). Furthermore, the text is considered especially relevant to ideas about deception and ambiguity (and it quotes Sun Tzu), given the emphasis on how to defeat an adversary without directly fighting and the notion that war is dynamic and cannot be tied to a static, predetermined plan. War is also about 'using all means', including armed force or non-armed force, military and non-military, and lethal and nonlethal means to compel the enemy to accept one's interests (see Qiao & Wang, 1999, p. 7).

Thus, overall, war is not seen as confined to the traditional military sphere and has been affected by technology. Therefore, the boundaries of the battlefield have expanded with the scope and scale of non-military means and non-military personnel all involved in competition. There is no apparent arena of contest that cannot be engaged with by employing a military mindset, while existing international laws and norms are prohibitive to upcoming powers such as China and exist solely to retain Western control and dominate it (Qiao & Wang, 1999). The text also touched on the ubiquitous nature of the internet and the impact of the RMA in enhancing both the reach and impact of battlefield tactics and enhancing asymmetrical or multidimensional attacks (Bunker, 2007).

Further, *Unrestricted Warfare* asserted that as technology progresses and outstrips the rate at which warfare doctrine advances, the line between non-warfare domains and warfare domains will increasingly blur. The perspective is that China is incapable of directly challenging the US in a military confrontation but it should restrict itself when thinking about how to win wars, which is akin to overlapping ideas by others postulating that 'one hacker + one modem causes an enemy damage and losses equal to those of a war' (see Qiao & Wang, 1999, p. 199). Such a blanket assertion in cyberspace could speak to the immaturity of some interpretations that appear to be vastly overestimating the capabilities of offensive cyber operations. However, the authors postulated that the only way to 'level the playing field' is via asymmetric tactics, and arguably, *Unrestricted Warfare* then has also positioned the Chinese perspective as one in which they are already victims of warfare tactics in various domains.

However, in critique of *Unrestricted Warfare*, its status as an unofficial document remains paramount (see Mattis, 2015). In addition, its analysis offered little insight into how the Chinese military might actually carry out war or how it will specifically utilise cyber methods to protect and promote Chinese interests (Mattis, 2015). Much of the book is commentary on history, notably the first Gulf War, and it discusses how war has changed but does not propose solutions to it in any solid or cohesive form (Baughman, 2022). As expressed at the beginning of the section, *Unrestricted Warfare* is fascinating as a document from officials writing in unofficial capacity on the nature of strategic thought and the evolution of warfare itself. This is useful information as a potential window to the thoughts that might inform or influence a more formal policy. Yet, useful as this may be, it does not carry the same level of insight offered by official government papers such as the SMS, which observers including Mattis (2015) have cited as far more significant in understanding official Chinese strategic thought.

3.4 Science of Military Strategy

As mentioned, *Unrestricted Warfare* is not a publicly endorsed research paper that underpins CCP military policy. For that measure, there is the SMS published through the Academy of Military Science located within the PLA (see Wuthnow, 2019).

Unlike *Unrestricted Warfare*, the SMS is the product of dozens of researchers based at this Academy—the highest-level research institute of the PLA—which reports to the Central Military Commission (CMC; Mattis, 2015). Thus, the SMS is much more indicative of the official Chinese military position on how conflict might shape in the future and on advancements in high-tech fields. The SMS often even aims to organise overarching operational and strategic focus into distinct concept categories such as power and stratagem, technology and skills, dispositions and capability, and yin and yang (balance in competition) in the incorporation of advanced technology into military operations and command structures (Thomas, 2014).

One limitation in utilising this text is that accessing an accurate English translation that has no inconsistencies and errors can prove to be difficult. Nonetheless, the importance of the text is demonstrated by authors who have argued that such documents do capture doctrinal development, technological innovation and strategic reforms backed by the CCP, including the employment of military forces at both tactical and strategic levels and the development of concepts such as offensive cyber operations (Mattis, 2015). For instance, in 2020, the SMS

stated that offensive and defensive cyber technologies have become the new 'commanding heights' of military competition:

> With the rapid popularization and continuous upgrading of network applications, military conflicts in cyberspace have also developed rapidly from simple to complex, from low-level to high-level, and the role of cyberspace military conflicts is increasing, as the futurist Toffler predicted; whoever has mastered the information and controlled the network will own the whole world. (China Aerospace Studies Institute, 2020, p. 148)

In other words, concepts such as peace in cyberspace are becoming more and more blurred as it has evolved into a fifth-dimension battlefield after land, sea, air and space—that is, the cyber battlefield (China Aerospace Studies Institute, 2020, p. 150). In short, 'peace and war are vague, and peace and war are connected' (China Aerospace Studies Institute, 2020, p. 150).

Military conflicts in cyberspace are also seen as characterised by multiplicity, relativity low investment and high efficiency: 'Military conflicts in cyberspace are mainly carried out through viruses and hackers, and these methods have unlimited diversity, so that cyber confrontations can surpass the limitations of other space military conflict' (China Aerospace Studies Institute, 2020, p. 151). For example, information warfare is seen as a significant portion of the overall military modernisation platform and a centrepiece in concepts such as deception and asymmetric warfare, which are often advanced by promoting high-achieving students through relevant university level courses with the intention of exploiting the resultant expertise in an information warfare environment (Department of Defense, 2002, p. 31). In terms of attribution challenges, it was argued:

> especially with the upgrading of network intrusion technology, more and more high-tech attack methods are very concealed, leaving no clues. It is difficult for the attacked to determine where the attack came from, and it is even more difficult to determine the true intention and strength of the attacker, and it may even be possible to be attacked and afterwards not notice it. (China Aerospace Studies Institute, 2020, p. 151)

Therefore, strategic pre-positioning based on hidden actions seems to have become an increasingly notable aspect of military doctrine and practice, which then had little to offer in terms of 'being caught' and the real or perceived impact on escalation owing to such cyber operations in peacetime (Borghard & Lonergan, 2019). This line of thinking would encourage network reconnaissance, 'counter-reconnaissance' and both defensive and offensive cyber

operations that aim to shape potential information warfare competition and seize control of this battlefield space. Thus, 'Without cyber security, there will be no national security' (China Aerospace Studies Institute, 2020, p. 154)

As mentioned earlier, upon observation of 'smart' weaponry being deployed in Operation Desert Storm, the CCP began to prioritise the modernisation of its forces with the realisation of a combat ideology based on integrated operations, low costs and a high cost-effectiveness ratio, given high-tech conditions (Hagestad, 2012). Given this new type of space–time domain based on technological advancements, Chinese cyberwarfare development aims to contend for or maintain a certain degree of dominance in this space. It is seen as necessary to develop strategic guidance for active defence in cyberspace, in order to deter warfare and adapt to strategic circumstances.

In this sense, China and the US have seen their relationship characterised by a growing rivalry for dominance (and prestige) in the Indo-Pacific region, particularly regarding the South China Sea, which has also affected related allied US powers such as Australia (White, 2013). In broad terms, China has continued to concentrate on safeguarding its 'overseas interests', which it had expounded as early as 2005 in the SMS as essential in an era of logistics in which maritime states must employ strategies to 'actively develop comprehensive sea power' and 'expand strategic depth at sea' (Erickson, 2007, p. 1).

Hence, China has invested heavily and broadly in day-to-day deterrence operations, especially cyber, as it saw the cyber domain as providing unique opportunities as an asymmetric instrument for balancing (mainly US) power but also a way for different types of tactical planning such as interference and espionage (Borghard & Lonergan, 2019). Hence, Desert Storm, in particular, made the CCP realise that militaries must modernise to project power, incorporate new technologies into existing military doctrine and the advance of cyber power would be crucial to project strategic hegemony. For instance, a PLA General commented as follows regarding the challenges and importance of informational warfare:

> In near future, Information warfare will control the form and future of war. We recognise this developmental trend of information warfare and see it as a driving force in China's military and combat readiness. This trend will be highly critical to achieve victory in future wars (Anand, 2006).

Certainly, in part, it can be argued that the CCP has adapted cyber concepts to suit national and international conditions and that since 1991, the Chinese military has incorporated technical advancements into its decision-making and strategic thinking with publications such as the SMS embracing 'grey-zone' ideas and defending the frontiers of both the internet and physical national security (Cozard, 2016, pp. 2–3,). Such initial steps would eventually become seismic changes in how the state itself approached warfare—arguably informed by a cynical interpretation of the motivations of other states towards it—with both defensive and offensive cyber operations seen as becoming more commonplace as a tool for advancing Chinese interests, such as seizing comprehensive control of the battlefield.

3.5 Science of Military Strategy, 2013

China under the leadership of Xi Jinping in 2013 continued to emphasise war operations in cyberspace and maintaining cyber sovereignty. The 2013 publication of the SMS is also an important text that crystalises the growing sophistication in Chinese military and strategic thought in these areas (see Mattis, 2015). It can be considered a 'capstone' document on China's military strategy and strategic guidance. In this sense, the text has three major and distinguishing features:

1. It is constituted with the basic essential factors of ordinary theoretical works in the discipline, it builds a basic theory of strategy and it maintains the relative completeness of the theoretical *tixi*[1] system framework. This was an important undertaking in determining a new launch point for strategy across entities such as the PLA and implied that a systems-of-systems approach was being undertaken at the strategic level in the Chinese military establishment.
2. It persists in combining theoretical and practical qualities, which allows it to possess a high degree of strategy, depth of theory and powerfully current focused quality; and in terms of theory, it is able to expound and explain the major issues in the area of PLA military strategic guidance under new circumstances.
3. It gives prominence to the main theme of the era and the academic main thread of military strategic theory innovation development under the new historical conditions (China Aerospace Studies Institute, 2021, p. i).

[1] *Tixi*: A unified whole formed by a group of interacting, mutually constraining entities (Stone & Wood, 2020, p. 18).

The implication of the above is that the 2013 SMS is a calculated document with a generally sound theoretical underpinning designed to inspect and describe PLA shortfalls at the strategic level and then propose effective solutions to them. Importantly, the text made a commitment to further develop Chinese strategy in the cyber domain as a major security domain alongside nuclear and outer space (SMS, 2013, p. ii). Further, the paper clarified the importance of military struggle in this new network domain, as it 'has distinct features different from those of military struggle in other domains' (SMS, 2013, p. 238).

The paper dissected four key characteristics of cyberspace conflicts. First, it discussed the 'wide-ranging quality of the scope of struggle'. Effectively, this section covers how in the modern age digital technologies are the fundamental means by

> which people regularly understand the world and connect with one another … including telecom, electric power, traffic, banking and finance, and social security … Computer-centered network systems serve as the nerve centers of modern military forces and military activity, and interlink the various operational strengths … into an organic integrated whole, which is a decisive factor and basic condition in the transformation of the form-state of war into informatised war. (SMS, 2013, p. 238)

Thus, the text emphasised the pervasive nature of the fifth domain of warfare and commented on its relevance to both the military space and civilian entities. The section also emphasised the likely impact of operations through cyber means on broader society, which would affect these civilian entities and industries and then have cascade effects. Importantly, this section covered how concealment and pre-positioning are crucial to the cyberwarfare initiative in creating the conditions for effectively achieving strategic goals (SMS, 2013, p. 239).

Second, the text specially highlighted the 'concealed quality in the modes of struggle' that muddies the situation of conflict in cyberspace:

> Information networks are distributed extremely broadly, and contain countless network nodes, but any one network node can be used for executing an attack against another network node or network system. Thus, within network warfare, determining the sources of threat and the directions of an attack is very difficult, even impossible (SMS, 2013, p. 239)

It also does not appear that these assertions were made in the context of a specific, ongoing war and the authors of the paper appear to be arguing that attribution is so difficult as to be

practically irresolvable. This may speak volumes about the conduct and logic of Chinese state-backed cyber forces as:

> Thus, in the actual practice of network struggle, even if one knows the source or direction of a network threat, it will still be difficult to swiftly determine completely whether it is the act of individuals or is an organized state act, or is sabotage activity conducted by a terrorist organization or criminal group, and it will be difficult to clearly distinguish who bears the responsibility. (SMS, 2013, p. 239)

This section perhaps implied a lack of faith in attribution in 2013 in China's own abilities, or at least a greater faith in China's capacity for its cyber units to operate stealthily and without attribution. The section also emphasised deterrence-by-punishment mechanisms. Fascinatingly, the section later asserted that the interconnectivity of networked military systems and civilian systems and the ambiguity of network operations may have played a part in 'restricting the outbreak of a large-scale network war' (SMS, 2013, p. 240).

Third, the text refers to the 'low expense and high effectiveness in the cost of struggle'. This is perhaps the weakest section among the four, revealing that perhaps at this time Chinese cyberwarfare doctrine did not have a strong command of the concept of 'low barrier' to entry. It is correct in asserting that 'computer network operations only require small numbers of personnel and network computers to be conducted, and fairly low investment of funds enables achieving the anticipated operational goals' (SMS, 2013, p. 240).

However, the section then delved into the US having network supremacy and therefore greater reliance and culminated in an uncited example of the US Navy's Atlantic Fleet allegedly having command seized by 'one US Air Force first lieutenant, using only one personal computer and one universal modem' (SMS, 2013, p. 240). It can be asserted without even delving into the empirical basis of this claim that there is no clarity on what these terms even mean. For instance, does command authority mean Domain Administrator access? Is the Atlantic Fleet under one single network? Therefore, these appear to be unfounded claims and speak to the inexperience or guesswork of what is supposed to be a hard-headed white paper by a military academy. This section is also only a single paragraph section in length, reinforcing that the 'cost' section is underdeveloped in general and that the idea of 'low barrier' to entry is not well understood in the cyber realm.

Last, the SMS noted the ‘professional quality of the struggle strengths’. This section has interesting and important details about the quality of individual skills and the training required to conduct what is described as ‘network warfare’, that is, the ability to carry out ‘sabotage of the enemy’s network system and network information, while at the same time protecting friendly network systems and network information’ (SMS, 2013, p. 241).

In illustrating the pervasive nature of the cyber domain, the section still carries the principal assertions that cyberwarfare is a skills-based professional field; states cannot necessarily throw money haphazardly at technology without investing in human resources; and individuals must be competent, practiced and elite to exert a significant impact on the battlefield as ‘cyber weapons are difficult to use, requiring specialized [sic] skills to design and manage, and they are not uniform’ (Depp, 2020). Therefore, military confrontation in the network domain can be seen as ‘a comparison and trial of strength of opposing sides in terms of the knowledge, intelligence, and professional capability of the cream of network talent’ (SMS, 2013, p. 241). The section bears consequence in the frankness of Chinese strategists that there are limitations to a pure numbers advantage in its population, given that cyber warriors themselves are highly trained and specialised individuals. Then, this fact may be seen as offering some competitive advantages to states such as Australia that might have a relatively low population size but a high education base from which to recruit.

Furthermore, the 2013 SMS paper openly asserted that China had acquired vast offensive cyber capabilities known as ‘network attack forces’. Subsequently, China had divided these network attack forces into three distinct types, as described by McReynolds (2015) later as:

1. Specialised military network attack forces: military operational unit employed for carrying out network attack and defence.
2. PLA-authorised forces: teams of network warfare specialists in civilian organisations authorised by the military to carry out network warfare operations.
3. Non-government forces: external entities that spontaneously engage in network attack and defence but can be organised and mobilised for network warfare operations.

Currently, this has translated into a desire to establish and maintain cyber corporations, such as Lenovo and Huawei, in China, which are capable of competing with already established global actors (see Gewirtz, 2019). Furthermore, it has expanded the status and role of conflicts in cyberspace to incorporate economic espionage and a ‘rob, replicate and replace’ mindset

(see Demers & Evanina, 2020). Thus, the SMS in 2013 focused heavily on the central role of peacetime 'network reconnaissance'—that is, the technical penetration and monitoring of an adversary's networks based on points 2 and 3—and in developing the PLA's ability to engage in both peacetime and wartime network operations. Notably, SMS 2013 included the first explicit acknowledgement of Chinese 'network attack forces', or in other words, what is known as offensive cyber operations.

Overall, the 2013 SMS clearly stated that the scope of cyber activities was expansive and presented a wide range of ideas about grey-zone coercion and asymmetric competition. It is a sound attempt at a more specialised analysis of warfare operations, particularly in the cyber domain. It provided some prescient analysis on the actual difficulties of cyberwar, particularly at levels that would facilitate strategic-level effects such as those with which Libicki's framework deals. However, the 2013 SMS also still showed an immaturity in Chinese strategic writing and thinking, such as uncited tales of rogue lieutenants in the US Navy miraculously seizing entire networks of fleets and holding them at threat. These tales are odd anecdotes and do not align well with the more detailed and structured components of this document that demonstrated the room for the growth that China needed to assert itself as a cyber power.

3.6 Defence White Paper 2015

The 2015 Chinese DWP begins with the assertion that the Chinese people wish to maintain peace, pursue development and share prosperity, and that the growth of China is interrelated with benefits for the world as a whole (State Council Information Office, 2015). To achieve this end, building a strong 'national defense and powerful armed forces is a strategic task of China's modernization drive and a security guarantee for China's peaceful development' (State Council Information Office, 2015 p. 2). It is also in this DWP that the Chinese deliberately designated cyberspace a 'new commanding height in strategic competition among all parties' (State Council Information Office, 2015 p. 5).

Section 3 of this DWP also detailed the Chinese understanding of active defence, asserting that it is 'the unity of strategic defense [sic] and operational and tactical offense… and adherence to the stance that "We will not attack unless we are attacked, but we will surely counterattack if attacked"' (State Council Information Office, 2015, p. 9). The cyber domain offers numerous opportunities to launch operational and tactical missions that may have wider strategic effects, which can be realised currently in efforts such as pre-positioning on networks prior to any

major kinetic conflict to justifying the intrusion (see INSIKT Group, 2021). Again, the cyber domain is identified as a new threat vector, and it is asserted that dealing with such threats to its cyber sovereignty is necessary to 'maintain the common security of the world community' (State Council Information Office, 2015, p. 10). To this end, the Chinese military had also incorporated the concept and implementation of information warfare in the digital age, which included reconnaissance (C4ISR) connectivity, psychological warfare and 'rob, replicate and replace' (Cozard, 2016). At this stage of its strategic thinking, the Chinese state was emphasising its modernisation drive—'expediting the development of a cyber-force'—and that cyber will be an advantageous and indispensable tool in a multidimensional strategic deterrence posture.

In reference to the new 'commanding heights' in strategic competition, it should be noted that while the 2015 DWP did not overtly discuss 'offensive' cyber operations, such a possibility could be seen as justified as inherent in the concept of 'active defense' (State Council Information Office, 2015). Kania (2015) argued that by this logic, deterrence by punishment could be

> considered integral elements of the Chinese military's efforts to 'resolutely safeguard China's sovereignty, security and development interests' in cyberspace. The question then becomes what China perceives to be an attack, a question complicated by the ambiguities of intent and challenges of attribution inherent in the cyber domain.

More broadly, the RMA was seen as proceeding to a different and provocative stage. Therefore, the core stated objective in the DWP indicated that such dynamics had a significant impact on the international political and military landscape as well as national security arrangements,

> potentially jeopardizing not only national security but also social stability. The need to 'maintain social stability' (mentioned six times) is presented as a primary mission of China's armed forces, which are also directed 'to remain a staunch force for upholding the CPC's [Communist Party of China] ruling position.' By extension, the mission of this new cyber force would therefore be not only to safeguard China's sovereignty in cyberspace but also to defend CPC rule against any threats emanating from this new domain. The perceived imperative of controlling content considered a threat to the CPC's authority is implicit in the concept of information security which is broader than cyber security or network security. (Kania, 2015)

Thus, given the need to build a strong national defence as a strategic task of China's modernisation drive, the 2015 DWP provided a basis for China's multidimensional strategic posture that included elements such as offshore defensive and offensive operations, which were intertwined with its civilian policy, economic growth and infrastructure development.

In regard to security concerns and cyber competition with major powers, the 2015 DWP positioned China as a purely reactive actor with benign strategic intentions in noting that it was 'one of the major victims of hacker attacks … confronted with grave threats to its cyber infrastructure' (State Council Information Office, 2015, p. 14). While adding that all nations were re-adjusting their security and military strategies and military organisational structures, given technological developments, it noted that China's more negatively focused security arrangements must 'expedite the development of a cyber-force,' and enhance its capabilities in 'cyberspace situation awareness', all issues complicated by the challenges of attribution in the cyber domain as seen in 2015 (State Council Information Office, 2015, pp 14-20).

These statements were made in the 2015 DWP despite evidence of more aggressive cyber activity, more proactive Chinese cyberwarfare and espionage actions abroad and the advancement of specialist units (see below) established in the PLA and the MSS , which hinted at an offensive orientation. As Uren (2020) argued:

> One well-documented example shows that the Jiangsu bureau of the China's Ministry of State Security carried out a multi-year combined cyber espionage and intelligence-gathering campaign to steal technology used in making components for the domestic airliner being built by the Chinese state–owned aerospace company Comac. This reportedly included successful compromises of companies such as Ametek, Honeywell, Safran, Capstone Turbine and General Electric, each of which makes jetliner parts.

Moreover, the strong advocacy of the concept of network sovereignty in 2015 aligned with notions of offensive behaviour that instead were being portrayed as inherently defensive in intent. It is worth noting that Major General Dai Qingmin, then director of the PLA's electronic warfare department, previously spearheaded the PLA's information warfare strategy. He later advocated a 'comprehensive information warfare effort' that incorporated offensive as well as defensive cyber operations (see Townsend, 2019). This sentiment represented a hawkish break away from the more diplomatic 2015 DWP policy that promised that China was 'opposed to interference in the internal affairs of others' (J Li, 2019) . Yet, as mentioned, a more offensive cyber posture to perceived threats against China's cyber sovereignty can be seen as

camouflaged within a term such as ‘active defence’, which is a characterisation that could certainly entail ideas that rationalise offensive information warfare operations and promote pre-emptive attacks in order to gain initiative and strategic advantage (see J Li, 2019).

Certainly, while conducting the integral role of peacetime ‘network reconnaissance’, such cyber operations can also be developed into both a credible first strike and counterstrike offensive capability, with civilian infrastructure as a legitimate target. As M Singh (2020) asserted:

> China believes that by achieving ‘cyberspace superiority’ it can deter or degrade an adversary’s ability to conduct military operations against China and manage the escalation of a conflict. Also, this enables China to scale these attacks to achieve desired conditions with minimal strategic cost and that using cyber-attacks demonstrate capabilities and resolve to an adversary.

One other notable development in 2015 was the idea of ‘force development’ in critical security domains, which emphasised cybersecurity and cyberspace as ‘a new pillar of economic and social development, and a new domain of national security’ (State Council Information Office, 2015, p. 14). Here, China again claimed that it is ‘one of the major victims of hacker attacks’, and therefore, as cyberspace ‘weighs more in military security, China will expedite the development of a cyber-force, and enhance its capabilities of cyberspace situation awareness, cyber defense [sic] … so as to stem major cyber crises’ (State Council Information Office, 2015, p. 14). This claim bears particular significance as it is the first Chinese DWP to assert the development of a ‘cyber-force’ with more security-focused interests and with the aim of preparing for future information warfare (see Erickson, 2019).

The 2015 DWP was a significant development point in China’s national cybersecurity strategy, which foreshowed a more competitive geo-strategic and cyber future. It served as a launch pad to justify an expanded cyber mandate as part of ‘active defence’. This mandate reinforced the right to adopt ‘force control’ and establish offensive cyberwarfare operations, especially as China felt these actions were justified owing to the external forces attacking the Chinese sovereign cyber domain (State Council Information Office, 2015, p. 14). It allowed a foothold for offensive concepts and a more proactive ‘active defence’ stance that focused on the shape and design of cyberwarfare operations. To this end, China witnessed an evolution to more agile hacking and associated collectives and a government-backed APT landscape targeting businesses and government organisations abroad. The secretive nature and intent of such threat

actors (as addressed below) remain highly relevant for Australia in its incident and deterrence response plans for addressing suspicious cyber activities, determining Chinese capabilities and establishing red lines for which attackerscan be punished by Australia for grievances.

3.7 General Staff Department, 3/PLA

The Third Department (3/PLA) of the PLA's Joint Staff Department was in charge of China's computer network operations, including intelligence gathering and network defence. This General Staff Department (GSD) also once contained much of the technical capacity for operations directed at foreign defence and industrial sectors and was responsible for monitoring communications for threats and commercial opportunities globally (see Areddy & Mozur, 2014). As stated, the unit, among other things, focused on collecting conventional intelligence on political and economic aspects of foreign governments, NGOs and opposition groups outside China (e.g. the Dalai Lama is a significant target; Areddy & Mozur, 2014, pp. 61–62).

Significantly, 3/PLA is seen as having contributed to operations for cyber espionage and theft, which some US military figures have described as a contribution towards 'the greatest transfer of wealth in history' (Rogin, 2012). These operations involved the pilfering of intellectual property from various Western commercial entities, which was then used for manufacturing in China, in the aforementioned 'rob, replicate and replace' strategy (see Gewirtz, 2019). But interestingly, in 2016 the CCP's official newspaper *People's Daily* emphasised the importance of centralised command for cyber operations in order to reduce the risk of escalation (Yi, 2016). In this sense, 3/PLA can be seen as reflecting the PLA's attempts to resolve prior combat-oriented deterrence issues and to build its cyber forces to ensure a separation of cyber espionage and offensive capacity. Thus, it appears that cyberwarfare units were organised according to the type of mission, for example, attack or defence.

In addition, the Intelligence Bureau of the Joint Staff Department, formerly the 2/PLA under the GSD, has been considered the premier Signals Intelligence (SIGINT) organisation of the PLA (see Pangburn, 2014). This domain-centric department also had two particularly notorious units integrating peacetime and wartime activities, Unit 61398 and Unit 61486, which were accused of carrying out cyber operations related to aerospace, satellites and related digital communications.

3.7.1 Unit 61398

One of the first cyber units attributed to China was the Second Bureau of the Third Amy, or Unit 61398, by FireEye in 2013 (Council on Foreign Relations, n.d.). Unit 61398, which is also referred to as Advanced Persistent Threat 1 (APT 1), was a Shanghai-based organisation that was arguably the most prolific and active unit of cyber attackers worldwide and has been constantly attributed directly as a state-sanctioned cyberwarfare actor that was part of PLA's cyber-espionage and technical reconnaissance capabilities (see Mandiant, 2013). Private cybersecurity firm Mandiant (2013, p. 3) has even alleged it was able to track down the official command units and their operations with enough precision to attribute the exact location to Datong Road in Gaoqiaozhen, Pudong New Area of Shanghai. Other names for the personnel working there are either Comment Crew or Shanghai Group (T Phillips, 2013). In response, Chinese authorities have consistently denied any connection between its military and cyber-espionage actions.

This level of public precision by Mandiant is especially useful in not only revealing Chinese operations but also signalling the attribution capabilities of countries such as the US and Australia. Often, secrecy is paramount to China for its cyberwarfare operations, and the displayed ability to accurately identify locations and especially persons involved in cyberwarfare activities can influence the strategic considerations and calculations of Chinese decision-makers. Mandiant (2013) also estimated that Unit 61398 used more than 1,000 servers. Such considerations are relevant to the discussion in Chapter 4 and ultimately to the ability of Australia to accurately determine the actors who have launched a cyber attack and to respond appropriately, including through deterrence by punishment. Yet, as stated, to date China's typical response to attribution and identification has largely been denial and it has asserted that such precise attribution is unattainable (Z Li, 2014; Reuters, 2023; Segal, 2015).

Nonetheless, the unit with its origins in China was largely involved in 'spear-phishing' espionage practices, primarily for establishing access to networks to steal vast quantities of data related, but not limited to, technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists, often by targeting the leadership structures of victim organisations (Mandiant 2013, p. 3). The main aims of this unit were

> to steal the most vulnerable information about developmental trends, economy, technology and research especially in the area of military industry or data about the strategies and doctrines of potential adversaries. These activities are aimed at gaining advantage over other countries in the region and in the world, developing the operational advantage in case of a potential armed conflict. (Kozlowski, 2015, p. 165).

In addition, hacking IT technologies in important industries appears to have been not only a core mission of the unit, but also an activity at which it was systematically skilled. Mandiant (2013, p. 3) asserted that APT1 had often maintained access to targeted networks for an average of 356 days and that the longest period was an incredible 1,764 days, or four years and 10 months before initial detection. The extensive state-based support necessary for such network defence and exploitation efforts would require large investments and highly experienced specialists such as linguists, malware authors, open-source researchers and various other roles invested in the translation of requests to operators and then translating stolen data to those who made the request (Mandiant, 2013).

These claims by Mandiant were verified by the US indictment of five PLA officers in 2014. The US argued they were all members of Unit 61398 and had all committed serious cyber-espionage activities (US Department of Justice, 2014). These particular activities had targeted six US citizens in nuclear power, metals and solar products industries. Former Attorney-General Eric Holder also asserted that these were the first ever charges laid against known state-sponsored actors for infiltrating US commercial targets by cyber means (Tiezzi, 2014). Then Assistant Attorney-General John Carlin also noted that the Chinese hackers stole trade secrets, designs for nuclear plant components, and cost, pricing and strategy information from private entities at the same time that Chinese competitors were acting to drive the same entities out of the market, which is a classic ‘rob, replicate and replace’ scenario (Tiezzi, 2014). The charges were also important for signalling attribution capabilities and the identification of the individuals involved with a ‘secret’ unit, indicating a new confidence from the US in their attribution profile (US Department of Justice, 2014). This signalling strategy may have affected Australia’s active involvement in future US writs against Chinese hackers who were seen as having a clear espionage-driven agenda.

3.7.2 Unit 61486

Unit 61486 was a PLA unit dedicated to cyber attacks, online spying and stealing trade and military secrets from overseas targets. These operations posed a considerable threat to

Australian critical infrastructure as China indicated that it understood networked operations in cyber space not only as a tool to deterrence but also as important for national campaigns to help it build its conventional armed forces more rapidly while increasing the competitiveness of Chinese entrepreneurship globally.

Unit 61486, according to CrowdStrike (2014), was headquartered in Shanghai and was a part of the 12th Bureau of the PLA's 3rd GSD. The unit specifically focused on attacks on foreign satellite, aerospace and communications industries to support China's space surveillance network. It is also known as 'Putter Panda' (CrowdStrike Global Intelligence Team, 2014).

Overall, the origins of this unit appear to indicate the recognition that the CCP needed to improve its information control capabilities by investing in satellite and aerospace technologies and stealing related information. The unit itself is believed to have been active since 2007 as one of China's avenues for military modernisation, although the secrecy surrounding it makes determining this unit's exact start date and maybe its end date difficult (see Saarinen, 2017). Nonetheless, CrowdStrike's forensic investigation through attribution concluded that parts of the unit's toolset had seen the unit identified as part of the MSUpdater Group, a cyber-group that deployed custom malware and that focused on exploiting productivity apps such as Adobe Reader and Microsoft Office (Crowdstrike Counter Adversary Operations, 2014). Such tools are utilised to target government, defence, research and technology sectors and satellite and aerospace industries (CrowdStrike, 2014, p. 4). CrowdStrike added that attribution is 'a key component of cyber-intelligence, by knowing the adversary you can effectively understand their intentions and objectives' (Counter Adversary Operations, 2014).

Further, CrowdStrike even attributed the domain registration for the command and control of the unit to a specific Chinese national, Chen Ping, also known as cpyy (Counter Adversary Operations, 2014). The unit was once again identified as based and operating in Shanghai and appeared to share much of the same infrastructure as Unit 61398. For instance, the remote access tools they had developed had enabled 'Putter Panda' to conduct intelligence-gathering operations with a high level of persistence on victim networks. The unit itself can be seen as emblematic of pre-positioning Chinese offensive capabilities by establishing access on victim networks that can be exploited, potentially to the point of unleashing capabilities that deliberately damage or degrade the targeted networks.

3.8 General Staff Department, 4/PLA

4PLA was a clandestine unit responsible for electronic warfare. It was considered the central offensive cyberwarfare unit for China, and similarly to 3/PLA, was dispersed into the Strategic Support Force (SSF).

The unit was again attributed to be based in Beijing and has been considered one of the more aggressive cyberwarfare agencies because of its mandate for high-technology warfare and sensitive intelligence gathering (see Gertz, 2017). 4 PLA, also known as the Electronic Countermeasures and Radar Department, had a clear mandate to launch offensive cyber attacks in the development of China's national cybersecurity strategy (Gertz, 2017). Concurrently, some sources within China stated that the unit was primarily defensive in nature. However, even some Chinese scholars and military commanders have openly admitted that this is a very ambiguous area and that it is especially difficult to determine peacetime and wartime in particular operating circumstances (Hsiao, 2010).

Certainly, it might be possible that some official CCP stipulations about the defensive nature of the unit indicate the new strategic 'active defence' positioning that China has undertaken, whereby the CCP has openly argued that these operations are merely active defence and that victim states are misinterpreting its actions. However, other evidence suggests that 4 PLA was first and foremost focused on the disruption and denial of enemy computer networks, which in itself would require extensive surveillance capabilities (see Gertz, 2017). Possibly, such PLA surveillance capabilities are no longer as important to Libicki's (2009) framework, given the growth of the MSS (see below). Nevertheless, strategic cyberwarfare, especially the notion of 'computers against computers' is today in the domain of the MSS which, as of the time of writing this thesis, has been taken from the PLA. APTs have a much firmer bearing in the civilian domain and now constitute a significant part of the CCP's cyberwarfare capabilities that would occur within the strategic cyberwarfare operations that Libicki specified.

3.9 PLA Cyberwarfare Evolution in Preparation for the Strategic Support Force

As mentioned, the PLA underwent significant policy changes and capability development in 2015 to 'active defence', which drastically changed the political and technical approach to its cyberwarfare and cybersecurity landscapes. The PLA had tended to focus on kinetic warfare

operations while ‘computer on computer’ cyberwarfare operations had moved to other entities such as the MSS.

Yet, the PLA still has a considerable number of cyber units to assist in information dominance and in shaping battlefields. The PLA has consistently ‘advocated cyber warfare to achieve a range of operational objectives, such as targeting an adversary’s command, control, and communications (C3) and logistics networks to hamper its ability to generate combat power during the early stages of an armed conflict’ (Ng, 2020).

As mentioned, in part because of the ‘lessons’ of Operations Desert Storm in 1990–1991, much of China’s military underwent significant technical, cultural and logistical changes, to some extent, to protect Chinese networks and to ensure its cyberspace superiority (see Farley, 2014). Indeed, a report compiled for the US-China Economic and Security Review Commission in 2018 on China’s cyberwarfare capabilities highlighted that the PLA poses a credible threat to US military and allied operations in the event of a conflict in the Indo-Pacific region. This report stated that the PLA ‘was gearing up for information confrontation and is seeking to integrate all elements of information warfare, electronic and non-electronic, offensive and defensive, under a single command authority’ (Ng, 2020). As covered later in Section 3.13 on the 2019 DWP, the Chinese often lump Australia into US considerations as well, acting as though Australia is constantly in lockstep with the superpower (State Council Information Office, 2019, p. 3). Effectively, because of the perceived arraignment of Western powers against it, China embarked on a mass modernisation program of its forces in order to launch counterattacks on various foreign organisations and governments.

In terms of cyber reorganisation, the result was that the four major departments of the PLA were dissolved, and instead, the bulk of the PLA’s functions was incorporated into various new organs within an expanded, more centralised CMC (McReynolds & Costello, 2018). The GSD became the new CMC Joint Staff Department, the General Political Department became the CMC Political Work Department, the General Armament Department became the CMC Equipment Development Department, and the General Logistics Department became the CMC Logistics Support Department (McReynolds & Costello, 2018). Specifically, the third and fourth units of the PLA, which were under the GSD, were the network warfare operations of the PLA, and these were absorbed into the new SSF, as discussed next.

In 2015, Beijing created what was seen as a counterpart to the US Cyber Command Centre—the SSF—which effectively combined the resources of the PLA in the field of cyber, space and electronic warfare. This new force structure is believed to be responsible for facilitating, in part, the integration of the PLA's cyberwarfare capabilities. As Costello and McReynolds (2018) revealed, the SSF has two primary roles, namely, strategic information support and strategic information operations:

> The SSF's strategic information support role entails centralizing technical intelligence collection and management, providing strategic intelligence support to theater commands, enabling PLA power projection, supporting strategic defense in the space and nuclear domains, and enabling joint operations. The SSF's strategic IO [Information Operations] role involves the coordinated employment of space, cyber, and electronic warfare to 'paralyze the enemy's operational system-of-systems' and 'sabotage the enemy's war command system-of-systems' in the initial stages of conflict (p. 2).

In December 2015, President Xi Jinping publicly remarked during the SSF founding ceremony that the SSF was a 'new-type combat force to maintain national security and is an important growth point for the PLA's combat capabilities' (Cordesman, Burke, & Malot, 2019). As mentioned, the PLA decided to construct the SSF as a separate service largely in order to develop a more focused cyberwarfare force and this decision was

> ostensibly driven by lessons learned from observing foreign militaries and is intended to avoid redundancies in force development and counterproductive rivalries for funding and resources … the SSF embodies the evolution of Chinese military thought about information as a strategic resource in warfare, recognizing both the role it plays in empowering forces and vulnerabilities that result from reliance on information systems. (McReynolds & Costello, 2018, p. 3)

In other words, the consolidation of information operations under the SSF was motivated by ideas aiming to execute specific types of strategic missions that key Chinese policymakers believed would be decisive in future major 'informatized' wars (McReynolds & Costello, 2018). Thus, China set about to develop its ability to launch offensive information operations rapidly and to protect its strategic frontiers, including cyber, by potentially moving beyond systems and structures that simply collected data for traditional state espionage. 'China is not reinventing the wheel, it's not creating whole new organizations. It has built the SSF with bricks, not clay, pulling and consolidating the force from previous existing organizations and

renaming them' (Costello, 2017). This revamped command and control of information operations appears to have centralised most PLA space, cyber, electronic and psychological warfare capabilities under a comprehensive, united umbrella as the PLA sought to pivot from land-based territorial defence to extended power projection for protecting Chinese interests in cyberspace (McReynolds & Costello, 2018).

3.10 Ministry of State Security

In terms of state-aligned or state-sponsored cyberthreats emerging from China, one of its most powerful intelligence services is the MSS. Investigations of MSS intrusions revealed that it has been involved in carrying out extensive hacking campaigns to steal data from government agencies and companies in various countries, including Australia (Galloway, 2021). In fact, in 2021, Australian Government joined other international partners in expressing 'serious concerns' about explicit malicious cyber activities citing China's MSS:

> In consultation with our partners, the Australian Government has determined that China's Ministry of State Security exploited vulnerabilities in the Microsoft Exchange software to affect thousands of computers and networks worldwide, including in Australia. These actions have undermined international stability and security by opening the door to a range of other actors, including cybercriminals, who continue to exploit this vulnerability for illicit gain (M Payne, et al., 2021).

Nonetheless, an important distinction is that the MSS is a civilian-based agency that constantly aims to distance itself from military and associated units as it operates through multiple layers—which do include affiliated media or commercial firms (Lyngaas, 2018). Nevertheless, this opaque structural and organisational posturing has enabled China to publicly split its cyber operations into different and siloed streams although, in practice, all Chinese tech companies retain close security and control connections to the CCP and the military (Bhattacharjee, 2023).

Significantly, the MSS can conduct integrated warfare operations such as electromagnetic spectrum warfare operations, cyberwarfare operations and space operations. More nuanced, intricate cyber operations that rely on stealth and data pilferage, the corruption of corporate and public cyber systems and general industrial espionage are also within the realm of the MSS (Lyngaas, 2018). In short, the MSS conducts operations that would certainly fit into modern definitions of cyberwarfare, and such actions represent the significant cyber dangers to Australian enterprises, both public and private. In addition, examples of APT activity that

would fall under the banner of the MSS's international activities include APT 10 and APT 3 (see Sections 3.10.1 and 3.10.2). Such entities are representative and typical in that they consistently pilfer intellectual property and conduct surveillance on foreign entities. Of course, such types of espionage do not automatically relate to strategic cyberwar concepts in Libicki's (2009) framework; rather, these are operational. However, the ability to penetrate networks in such a clandestine fashion and manipulate data is also an essential component of perpetrations for more offensive cyber operations.

3.10.1 APT 10

APT10 is a state-sponsored Chinese hacking group that has been active since at least 2009 (FireEye, 2017). It has targeted a diverse array of commercial activity, industries and technologies in Australia and across much of the globe.

Attribution and evidence for its cyber-espionage campaigns and data theft were uncovered in 2018 when the US publicly called for the arrest of two Chinese individuals for intellectual property theft. The US accused the state-sponsored hacking group of having breached computer networks in a broad range of critical US industries, including aviation and space and pharmaceutical technology (Tiezzi, 2018). Likewise, following the US statement, the Australian Government also demanded that the CCP shut down hacking groups that had been engaged in stealing intellectual property from various Western countries—albeit not APT 10 or the two individuals specially although the scope of Australia cyber concerns did fit within APT 10's typical cyber-hacking activities (M Payne et al., 2021)**.**

However, the US provided details and alleged that the members had been active from at least 2006 up to 2018 and had conducted various global campaigns of computer intrusions targeting intellectual property and confidential business and technological information at managed service providers, which are companies that remotely manage the IT infrastructure of businesses and governments worldwide (US Department of Justice, Office of Public Affairs, 2018). The US noted, 'It is galling that American companies and government agencies spent years of research and countless dollars to develop their intellectual property, while the defendants simply stole it and got it for free' (US Department of Justice, Office of Public Affairs, 2018). However, these individuals did not face US imprisonment as they were not in US custody, nor did China extradite them, but the signalling effect as regards attribution was apparent.

Consequently, the importance of these public accusations was a communication of robust attribution processes—which will be discussed in the next chapter—and a political message about how seriously the US and its allies such as Australia would consider such criminal conduct and related hacking cases. It indicates a growing 'name and shame' mentality, which was also repeated by successive governments from the Morrison Government to the Albanese Government, as indicated in the prior chapter.

FireEye (2018) also asserted that APT 10 was tied to the MSS and had historically targeted engineering aerospace, telecom firms and various governments to support Chinese national security goals, which include acquiring valuable military and intelligence information and the theft of confidential business data. Suffice to say, APT 10 appears a significant and pervasive cyber-espionage unit heavily involved in the extraction of intellectual property for the purpose of 'levelling the playing field' between China and potential competitors both in the public and private arenas. In short, APT 10 again appears to embody the cyber strategy of 'rob, replicate and replace' or at least fulfilling the crucial first step: rob.

FireEye has also provided a useful example of the APT 10 approach, which, at a basic level, seems relatively 'unsophisticated'. The attack overview revealed that APT 10 often began its operations with a simple phishing email (where the attacker sends an email with malicious attachments or links). The email enticed potential victims by including links in the local language that appeared to be articles on topics such as maritime and diplomatic issues and North Korea. Eventually, the target system had a quiet executable running, which appeared to be a legitimate pre-installed Windows program (FireEye, 2018). Thus, 'unsophisticated' methods such as phishing have proven highly effective at enabling APTs to gain access to networks, including those owned and controlled by public and private Australian entities (FireEye, 2018). In 2018, the Australian Government again named the MSS and called on China to honour a pledge it had made at the G20 Leaders meeting in 2015 (and at a subsequent bilateral meeting in 2017) to refrain from such hacking and cyber theft (see M Payne et al., 2021).

3.10.2 APT 3

APT 3 is another example of a China-based espionage actor that focuses on targeting aerospace and defence, construction, high-tech, telecommunications and transportation organisations (Saarinen 2017). APT3 is linked to Chinese intelligence and was the group seen as solely

responsible for a hack in 2013 in which the blueprints for the new ASIO building in Canberra were stolen through malware (Grubb, 2013).

In order to execute such a hacking spree, the group deploys browser-based zero-day exploits to exploit a target host; essentially, attacks are launched by exploiting vulnerabilities in the very web browsers their target victim utilises (FireEye, 2015). However, similarly to all APTs, the group will also deploy other intrusion methods should they be more suitable—it would appear that this particular technique is a distinctive feature for the APT. The group also utilises phishing campaigns, often sending .pdf files to target victims and exploiting those who click on suspicious links (FireEye, 2015).

Further, APT 3 is often referred to as a company called Boyusec, which has been identified and tied to the MSS and helps it accelerate its cyber-espionage activities and bypass foreign security measures (Gertz, 2016). Moreover, the APT has also been linked closely to Huawei, an entity with some notoriety in Australia for it is banned by the government from rolling out across Australia's burgeoning 5G network (McGuirk, 2022). Indeed, it is worth noting that Australia was the first nation to rebuke Huawei in such a fashion and owing to pressing security concerns. This ban was a public demonstration that confidence in attribution from the former Morrison Government had then led to a punitive policy and political response (Clark, 2021).

Furthermore, the group has also been blamed for observing and replicating US National Security Agency (NSA) cyber weapons that had been deployed against suspected NSA targets (Vavra, 2019). Check Point alleged that the group could have replicated these weapons by simply observing the systems under attack by the NSA, which itself speaks to a high level of capability. Of course, this capability is then augmented by the addition of another weapon to the arsenal, thanks to observing the NSA weapon in action. The observation could have taken place by being either a victim or a fortunate observer of the system the NSA attacked, or even by setting up a machine to be deliberately attacked by the NSA and recording the results, which is known as a honeypot operation (Vavra, 2019). Concurrently, APT3 has also been observed exploiting zero-day vulnerabilities in operating systems such as Windows.

Significantly, all these vulnerabilities appear to be exploits developed by an entity known as Equation Group—that is strongly implied to be an actor controlled by NSA and involved in operations such as Stuxnet (Kaspersky Group, 2015). Hence, APT3 has been observed deploying Equation Group weapons well ahead of a significant data breach that then released

a trove of other Equation Group weaponry (Threat Hunter Team, 2019). The evidence that APT3 can replicate incredibly advanced cyber weaponry by observation, or even bait the weapons to be utilised against dummy targets, indicates an incredible development of Chinese cyberwarfare capabilities, which have arguably been advanced to the point that they are described as being capable of degrading core US and Australian operational and technological advantages (Otto, 2019).

At the very least, being able to replicate accurately and effectively what is considered the most advanced cyberwarfare group in the world hardly constitutes the actions of 'drunken burglars', as they were described earlier in the chapter (Kirk, 2016).

While APT3 appeared to 'go quiet' in 2017, more recent reports have indicated that the group is active again in the gathering of geopolitical intelligence (US Department of Justice, Office of Public Affairs, 2019). For instance, it has deployed a particular malware called Bemstour, and Symantec has found that Bemstour's development has continued in 2019, which implies that the APT remains active, although this information is yet to be confirmed (Threat Hunter Team, 2019). Nevertheless, it is important to note that the malware serves the purpose of acquiring a persistent presence on the victim's network and was repeatedly deployed over a long period with many adjustments in order to attempt to bypass the target's defences, which is a classic indication of APT behaviour.

Overall, the APT 3 group has shown consistently high capability and temerity in infiltrating a foreign government or related body. In this sense, China's cyberwarfare capability and its ability to launch a prolonged campaign against a state such as Australia and its society should be seen as comprehensive. It has been able to do so despite public warnings from nations such as the US and Australia to Chinese hackers and others, asking them to refrain from compromising foreign networks worldwide for commercial and political gains or leverage.

3.11 Defence White Paper in 2019

The 2019 *Defence White Paper: China's National Defense in the New Era* blamed other state actors, especially the US, for geo-strategic instability in order to justify China's military and cyber build-up and associated activities (Fravel, Hiim & Trøan, 2023; State Council Information Office, 2019). In short, it flagged that the US and China were now competing superpowers and presented CCP reactions to threats as defensive and peaceful.

The 2019 DWP also listed the missions and tasks that the PLA is to perform in the new era as ‘safeguarding national territorial sovereignty and maritime rights and interests’, ‘maintaining combat readiness’, ‘carrying out military training in real combat conditions’, ‘safeguarding interests in major security fields’, ‘countering terrorism and maintaining stability’, ‘protecting China’s overseas interests’ and ‘participating in disaster rescue and relief’ (State Council Information Office, 2019).

Thus, international strategic rivalry is seen to be increasing. Chapter 1 of the 2019 DWP, entitled ‘International Security Situation’, essentially describes the strategic context in which China finds itself, arguing that the ‘international security system and order are undermined by growing hegemonism, power politics, unilateralism and constant regional conflicts and wars’ (State Council Information Office, 2019, p. 2). Australia is also directly named, with its relationship with the US being cited, and also that Australia seeks a larger role in Western security affairs, which is undermining global strategic stability (State Council Information Office, 2019, p. 3). Further, cybersecurity is identified as a distinct, substantial security threat, as a part of growing global military competition, and thus, protecting cyberspace is designated as a core national defence aim (State Council Information Office, 2019 pp. 4–7).

However, cybersecurity does not receive a strong mention in the paper beyond some broad and general comments, and a paragraph in the chapter entitled ‘Safeguarding Interests in Major Security Fields’ again describes protecting sovereignty in cyberspace as major aspect of Chinese military activity albeit a peaceful pursuit (State Council Information Office, 2019, p. 13). The DWP also highlighted a new Chinese emphasis on ‘combat readiness and military training in real combat conditions’ (State Council Information Office, 2019, p.16)

Alternatively, despite the careful and open-ended wording of the text, a 2019 report compiled for the US-China Economic and Security Review Commission noted:

> China’s cyber warfare capabilities would pose a credible threat to US military operations in the event of a conflict in the Asia-Pacific region. The PLA, it said, was gearing up for ‘information confrontation’ and is seeking to ‘integrate all elements of information warfare, electronic and non-electronic, offensive and defensive, under a single command authority’. Other than offensive cyber capabilities, state-linked hackers have reportedly compromised the computer networks of US defence companies on multiple occasions, pilfering valuable data on classified military developments (Ng, 2020).

In other words, China has developed great expertise and sophistication in its understanding and execution of its information warfare techniques. Therefore, some commentators have argued that US should respond by 'strengthening its level of deterrence and its strategic partnerships in Asia' as well as in Australia (Cordesman, 2019). Significantly, the background of Chinese cyber intrusions also indicate that the CCP is gaining substantial practical and theoretical experience in 'peacetime'. In this sense, many strategic cyberwarfare units that are designed to exploit weaknesses in adversarial states are typically civilian units and are often geared towards non-warfare-oriented targets such as critical infrastructure (P Singh, 2023). APT's are, or can be, organised as seemingly legitimate businesses, although they might actually be intelligence agency's purpose built for maintaining these intrusions and aiming for plausible deniability (O'Neill, 2022).

3.12 Science of Military Strategy in 2017 and 2020

The 2017 SMS produced by the Academy of Military Science has since had updates added to it in 2020 (Wuthnow, 2021). For this reason, the paper shall simply be referred to as the 2020 SMS and the latest edition will be analysed, instead of treating the publications as two separate papers that both discuss cyberspace strategy.

The 2020 SMS that reveals Chinese military thinking is the longest, most intricate publication of the series. From the introduction, the paper asserts that 'the threats from the maritime direction have increased significantly, which has become the focus of military strategic guidance' but still recognises that 'security issues in the … network, electromagnetic and other fields have become increasingly prominent' (Academy of Military Science, 2020, p. 3). The 2020 SMS can be seen as the capstone document on China's current military strategy across a range of emerging technologies, 'and the text was prepared by China's Academy of Military Science faculty with very high-level review' (China Aerospace Studies Institute, 2022). AI, along with a range of other technologies, is again seen as changing the form of warfare.

Interestingly, the paper delves further into political machinations and its effects on warfare efforts, at least slightly further than previous iterations, including to promote military–civil fusion. The 2020 addition of 'wartime political work' in Chapter 10 asserts that the political work of the CCP is crucial in carrying out military operations, consistent with Xi Jinping's 'emphasis on improving party control over the military, but according to the 2020 SMS, the changing character of war itself influenced this discussion' (Wuthnow, 2021). Other

commentators have identified that China seeks to seize an operations advantage through initiative and transformation as part of the global RMA (Kania, 2021). These technologies constitute fields such as AI, machine learning and quantum computing that go beyond the scope of cyberwarfare for this paper (Kania, 2020, p. 2). Burke, Gunness, Cooper and Cozad (2020) found that the paper identified three concepts that will guide force development:

1. War control (and therefore campaign success) depends on information dominance.
2. Combat space is shrinking, but war space has expanded.
3. Target-centric warfare defeats the adversary's operational system. (p. 1)

Further:

> In the new era, the main research is the guiding principles of military force construction and development under the development of mechanization, informatization and intelligent integration; army, navy, air force, rocket force, military space force, cyberspace force, joint logistics support force, armed police force and reserve strength building and development trends, capacity requirements and main measures, etc. (Academy of Military Science, 2020, p. 6)

Continuing the integration of cyber capabilities alongside the arms of the state is a stated core objective in the 2020 SMS, furthering the political integration as discussed by Wuthnow (2021), 'including the need to explore a "new model" of "political work plus information and network operations"'. This objective aligns with the continuing use of cyber means to influence Chinese adversaries, or potential adversaries, owing to the view that network weapons and talent development pipelines include military weapons development and training programs. Further, the objectives for cyber coercion almost certainly include disrupting, damaging or destroying the function of military and civilian information systems and critical infrastructure (INSIKT Group, 2022).

Yet, this policy orientation is not drastically new to the objectives of previous SMS papers. Per Wuthnow and Fravel (2022), 'despite being described as the military strategic guideline of the CCP's "new era", the new strategy largely represents a rebranding or relabeling [sic] of the one adopted in 2014'. Indeed, the edits between the 2020 and 2017 versions of this paper may betray other intentions from China, as 'the 2020 edition contains fewer details about topics that are likely considered sensitive by the PLA censors, such as … offensive network operations' (Clay & Lee, 2022, p. 1). The paper then becomes light on detail and instead turns to vague

assertions that strategic research needing expansion, issues that need urgent research are increasing, research methods must continue to be innovated and strategic studies are closely related to other disciplines to enable the discovery of military patterns that may prove actionable (Academy of Military Science, 2020 pp. 6–8).

Despite this lack of detail, Clay and Lee (2022) asserted that 'the 2020 edition unmistakeably demonstrate(s) the growing confidence of PLA academics in their assessment of the PLA's overall military capabilities' (p. 2). The authors of the 2020 SMS still posited the benefits of active defence and also that Chinese military developments, including in the cyber domain, have continued to mature and are granting strategists more options to consider for the control of future operations (Clay & Lee, 2022). It also has some new concepts such as 'intelligentization', which broadly refers to a new phase of military modernisation by introducing new sophisticated technologies such as AI and big data analysis to military operations (Wuthnow, 2021). This will occur primarily through civil–military fusion, that is, by utilising private-sector capacity to develop technologies according to military needs (see A Brown, 2022).

Overall, the 2020 SMS is thought-provoking and provides some new insights as well as much of the same. However, it ultimately emphasises operational cyberwarfare over strategic cyberwarfare operations through entities such as the PLA. The paper itself emphasises that operational and tactical operations in cyberspace are critical to winning wars, 'without exception. The victory of the war begins with the victory of cyberspace' (Academy of Military Sciences, 2020, p. 150). A telling statement is 'Peace and war are vague, and peace and war are connected' (Academy of Military Sciences, 2020, p. 150). In this section, the authors asserted that the boundary between peace and war is blurred in cyberspace, that confrontational behaviour in the cyber domain is present in peacetime and war and, critically, that any country is in the process of being infiltrated and attacked—even in peacetime, the cyber domain presents a cyber battlefield that is a key area that will determine the outcome of warfare (Academy of Military Sciences, 2020, p. 150). Cyber operations have been tied into the objectives of military ones because of the pervasive nature of the cyber domain across public, private, civilian and military entities. Hence, the Chinese perspective is that cyber operations are furthering Chinese strategy and national interest, regardless of whether actions are conducted in peace or in war.

3.13 Conclusion

This chapter has argued that China has been steadily expanding its cyberspace resources and cyber capabilities towards becoming a major cyber power. Overall, the pursuit of military innovations is consistently understood as a priority and a national imperative and there is a blurring of the boundaries between peace and war. The evolution of China's ambitious cyber programs could also indicate how it might act in a conflict that incorporates political and diplomatic dimensions of warfare in its modernisation programs. Critically, a PLA tradition that has emphasised deception is highly relevant to Libicki's (2009) question, 'Do we know who did it?'.

China's denial and deception game is highly relevant to Australia's deterrence frameworks owing to the challenge of ambiguity in cyber attacks that continue to aim to subvert systems and networks. Again, as Libicki (2017) revealed:

> Ambiguity entails doubt over who is doing what and for what purpose. Cyberspace operations unfold in a dense fog of ambiguity (even as certain fogs that have bedeviled kinetic operations are lifting). In the wake of a cyber-attack, although context may provide a strong clue of who did what, attribution can be a problem if and when attackers take pains to mask their involvement. (p. 55)

China has also undergone significant investment in capability in the cyber domain, including for the conduct of offensive cyber operations such as APTs, which comprise advanced cyber units controlled both by its military and civilian entities. APTs appear to be very well-organised computer intrusion units that can utilise multiple methods and various tools to focus on technology or behavioural psychology exploitation in order to gain long-term access to digitally stored information (Riehle & May, 2019). It is particularly challenging to protect against state-sponsored IP theft performed using APT's—they typically appear to employ highly talented individuals that can utilise resources for extended periods, often without regard to the financial employment costs of the operation (Kaspersky, n.d).

In the backdrop of current geopolitical circumstances, in broad terms, Chinese strategies have tended to prioritise offence over defence, focusing on disrupting the capabilities of potential adversaries such as Australia and disrupting the ability of victims to create a clear vision of the landscape and respond appropriately. In particular, the SMS papers provided the broad strategic-level reasoning behind this rising geo-strategic competition with the US, and the

successive DWPs discussed in this chapter have also specified the operational requirements for the Chinese intelligence and warfare structures, which have been realised in the APTs that have proliferated in China and carried out global cyber operations.

These facts may indicate that China has a higher threshold for risk than Australia may expect or, in turn, have. This analysis of risk thresholds is also buoyed by Chinese impressions of aggression from the US with Australia in tow, as indicated in the 2019 DWP, which results in China further strengthening its cyber capabilities and justifying a more offensive strategy in deploying them. The feedback loop is that as Australia in turn develops cybersecurity tools and entities, China uses this as justification for its own more offensive operations: a classic security dilemma.

Therefore, and explored in more detail later, deterrence strategy that would affect strategic cyberwarfare efforts should focus on peacetime cyber operations by China as if they are operations that would prepare the Chinese for more kinetic warfare operations. At the very least, the evidence supplied throughout the chapter shows that Chinese cyber operations have become more pronounced, aggressive and sophisticated and are now also being deployed with future conflict in mind. Australian decision-makers will need to consider this aggression and risk threshold in determining deterrence by punishment tools of their own.

Critically, the chapter showed that the CCP blends its capabilities with criminal or indirect public networks to hide its identity. Hence, from an Australian perspective, Chinese strategy in cyberspace is to emphasise the capacity to quickly execute warfare functions highly enabled by the deployment of cyber tools. These cyber tools can be observed to be in a constant state of readiness, if not already deployed in pre-positioning operations that have been publicly attributed as operating since 2017 (INSIKT Group, 2021). The extant operations in the civilian domain may, in fact, be actively in the service of military efforts, or civilian espionage efforts, but are regardless treated with the same severity and the same strategic objective of maintaining Chinese independence and the capacity to assert itself in the region. The PLA perceives that the competition continuum has widened, and in order to achieve its political objectives, the PLA may become more prone to rely on the strategic use of force to access the coercion spectrum. However, this does not mean that armed conflict or war is imminent but, rather, that active defence is conducive to being ‘defensive against offensive enemies with active offensive actions’ (Clay & Lee, 2022, p. 2; also see Academy of Military Science, 2020, p. 31).

Therefore, the necessary next step for constructing a coherent and applicable deterrence strategy that can assist Australia against malicious actions by China will require investigating and confirming attribution capabilities that can help to inform Australia's ability to identify, respond and potentially punish assailants in strategic cyberwarfare scenarios, as discussed in the next chapter.

Chapter 4: Australia's Attribution 'Who did it' Capability and Strategy

4.1 Introduction

Attributing attacks, via public means or secretly (*sub rosa*), is crucial for Australia and its capacity to respond and deter effectively in the cyber domain against an actor such as China. Attribution is a fundamental part of a cyber-deterrence strategy, as it involves both the process and problem of determining the actors behind an attack. To combat cyberthreats and to justify and coordinate policy actions, sufficient evidence must be garnered, analysed and argued before decision-makers might then be able to mitigate the problem or to allow scope to 'pull the trigger' on a potential punishment by deterrence response (Libicki, 2009, p. 117).

This chapter will describe and examine the significance of attribution, the difficulties and challenges involved, the capabilities, including resources and skills, and related background knowledge for attribution that Australia has demonstrated. It will then apply and intertwine these issues to questions 1, 5, 6 and 8 from Libicki's (2009) framework (as stated in Chapter 1). It will also specifically focus on what can be termed 'government-to-government attribution', that is, attribution related to public accusations by the Australian Government that have (sometimes) openly named state actors such as China as responsible for a certain cyber anomaly or operation. The chapter leans on policy analysis to inform the research garnered, to better inform the Libicki framework and also with the intention of structuring the analysis of empirical material. Therefore, a systems analysis will be incorporated throughout, wherein the system model is clarified by defining the boundaries and subsequently the structure (Walker W, 2000, p. 13). In practice, the boundaries shall be the restriction of the case study for Australia and China strictly to the cyber domain, where attribution will inform cyber responses despite there no doubt being other options available to Australian decision-makers. By acknowledging that two sets of forces act upon the system – external forces outside the control of the actors, and policy changes – the forces affect the structure of the system (ibid, p. 13). In short, external forces impose uncertainty on policy and become catalysts for change. Public policy research must go beyond describing a problem or situation into engaging with the how and why of things. This has informed Australian cyber policy and attribution is no exception in the domain.

This analytical framework aims to raise the level of confidence in future assessments, inform ‘best practices’ for addressing cyber attribution and assist in avoiding likely problems, such as the risk of escalation in the context of the China–Australia relationship. These best practices can then be used to inform and support deterrence responses (e.g. retaliatory cyber actions) and the cost–benefit analysis associated with potentially deploying the use or threat of punishment frameworks against China in order to dissuade it (and, conceivably, other states) from carrying out certain types of cyber operations.

Attribution, namely, piecing together evidence to determine ‘who did it’ and ‘who is to blame’, is one of the most widely debated problems of an evolving cyber field, especially given the Chinese strategy of employing deception in cyber policy and outsourcing to maintain deniability (Chapter 3) as well as the underlying (and relative) anonymity and fragmented architecture of the internet (Develle, 2016; Lindsay, 2015; Rid & Buchanan, 2014). In other words, attribution will entail a degree of trial and error—an exploration of whether a detected cyber anomaly is the outcome of a deliberate malicious action or a more benign human or technical failure (Levite & Lee, 2022). Critical to Levite and Lee’s (2022) contribution to defining attribution is the view that if the cyber anomaly has been caused by malicious behaviour, the actor determined as responsible must be publicly exposed. The identity of the perpetrator and the context of ‘naming and shaming’ China, in particular, has been a recurring issue for Australian policymakers and directly informs part of the purpose of this chapter’s investigation.

Further, and explored in more detail later in this chapter, the challenge of attribution overlaps with possible issues of escalation and the need for private–public partnerships and proportionate responses based on a combination of political judgement and related technical information (Lindsay, 2015, p. 54). These debate points will also involve an assessment of whether any cyber anomaly represents a broader pattern of behaviour or conversely could be considered intermittent or even a one-off occurrence. As mentioned in previous chapters, Australia’s 2017 International Cyber Engagement Strategy supported both whole-of-government and international diplomatic actions to support an international architecture to mitigate and deter ‘unacceptable’ behaviour in cyberspace (Department of Foreign Affairs and Trade, 2017b, p. 54).

In broad terms, the general objectives of attribution are to track down, identify and hold accountable the cyber attacker and then to advance and support policy options, such as punishment, repair and deterrence. Thus, public attribution, as it relates to cyberspace, is

> a recent phenomenon whose purposes, effectiveness, and consequences are the subject of heated debate. Most countries – including those with formidable cyber capabilities like China, France, and Russia – have refrained from explicitly and publicly attributing cyber-attacks to specific foreign state-affiliated actors. Many of the most high-profile public accusations by governments have so far been made by the U.S.-led Five Eyes intelligence alliance (comprising Australia, Canada, New Zealand, the UK, and the United States) against major ideological adversaries like China, Russia, Iran, and North Korea (Chuanying, Perkovich & Yang, 2022, pp. 43-44).

In this context, the Australian Government has been relatively slow and hesitant in publicly advocating the attribution capabilities of its cybersecurity apparatus. However, since 2017, there has been a rapid uptick in the government's public reassurance of capability, which has moved from passivity to supporting a policy approach by naming and shaming cyber adversaries. This approach includes deliberate efforts by government agencies including the ASD to 'lead by example'. Indeed, since 2017, Australia has publicly attributed malicious cyber activity to various actors such as North Korea, Russia, Iran and China (M Payne et al., 2021). Consequently, an investigation of Australian attribution capabilities and its level of confidence in attribution as well as an assessment of China's intent will be essential in determining the nature of and capacity for deterrence mechanisms that Australia can use against China.

Overall, effective deterrence by punishment will continue to rely on the accurate and valid attribution of a cyber attack and on assessing the source or sponsor of a malicious activity once it has been discovered, in order to facilitate an appropriate, informed and cohesive policy response. Thus, attribution is crucial for effective mitigation and punishment, including to increase adversary costs after a cyber violation. As M Payne et al. (2021) stated, Australia's cybersecurity posture

> is strong, but there is no room for complacency given the online threat environment is constantly evolving. Protecting Australia from malicious cyber activity – be it by state actors or cybercriminals – requires a continuous improvement approach to cyber security practices across all levels of society including government, business and households.

4.2 Risk Assessments and Responses

Consequently, in efforts to build attribution capability and to improve the speed and integrity of an attribution, one of the principal barriers to successful cyber deterrence in Australia, given a setting that requires 'acceptable' proof to be provided, has remained the practice of accurate or credible attribution as part of a tailored response to cyber operations by China. Of course, the Australian Government may also combine any public response with diplomatic and associated actions taken in private. However, while acknowledging multiple policy tools, the chapter will primarily focus on Australian efforts to discover and communicate with a specific public attribution, in part, to increase the effectiveness and timeliness of response for deterrence options. Hence the Libicki (2009) starting point: Do we know who did it?

In the case of evidence-reliant attribution, either public or in private, significant challenges for cyber deterrence remain, given resource challenges and problems such as disproportionality, misattribution, false flags, plausible deniability and even a lack of consensus on standards of proof (Develle, 2016). Yet, as Eichensehr (2020) noted, 'understanding who the attacker is can shed light on intruders' likely targets and goals' (p. 556) and, as a result, help policymakers to both anticipate and prepare for a particular cyber actor's actions. From here, Australia could then decide whether public attribution is suitable or whether, as Libicki (2209) said, *sub rosa* communications may be more formidable (p. x). Eichensehr (2020) also asserted that attribution is an important policy tool for victim states communicating privately, which lowers the requirement for exhaustive evidence and imposes at least some political cost on attackers—at the very least, it may shape their behaviour and affect their strategic cost–benefit decision-making (p. 552).

This effort to align attribution with more tangible deterrence actions is closely tied to what is referred to as forensic attribution: the careful collection of evidence regarding a cyber anomaly and the use of that evidence to then prosecute a case (maybe in the public arena) and even encourage support or sympathy from allied domestic and global audiences. Yet, adding to the policy complexity for countries including Australia, it has been argued that no common and universally agreed standard 'exists today for establishing a degree of confidence in determining cyber attribution' (Banks, 2021; Iasiello, 2018; Lewis, 2022; Mueller, Grindal, Kuerbis, & Badiei, 2019; Yang, 2022). In contrast, despite lacking an internationally recognised, standard forensic investigation model that can be brought to a public court, attribution that is heavily reliant on evidence will still be useful for justifying responses, including in the use of

cyberwarfare actions and implements. Therefore, despite the lack of a universally accepted method of attribution, compiling enough evidence that can reassure decision-makers in deploying retributive actions will have to suffice. Ideally, this evidence should also be reassuring to Australian allies such as the US to satisfy alliance needs for a joint evidence-based response.

Another challenge associated with the difficulty of ongoing uncertainties and related risk assessments and responses to cyber incidents is the issue of delay and time lags in striking back, including diplomatically, at the perceived aggressor. In short, cyber investigations are considered highly resource-intensive and time-consuming (Skopik & Pahi, 2020). That is, as Goodman (2010) asserted, if policymakers can verify an attacker's identity, a thorough investigation of origins and motives 'may take quite some time; some so long that the counterattack seems more like aggression than retaliation' (p. 112). Alternatively, others have claimed that at least in the most advanced states such as Australia 'digital forensics and threat intelligence have evolved to the point that quick and reliable attribution of the machines responsible for cyber intrusions is the norm' (Banks, 2021, p. 1053).

The key to the Banks (2021) quotation is indicating the specific machines that have been used, which still presents another attribution problem to be overcome, and who operates these machines. This attribution and time problem manifests not only as those who physically sit at and operate said machines, as machines can be remotely accessed and potentially deployed in service of a cyber attack; for example, botnets are a common form of a remotely controlled machine used in service of a cyber attack (Radware, 2024). Therefore, even if Australia can claim the ability to attribute a machine quickly and reliably, it may still not be certain who has deployed that machine. Therefore, attribution remains both a political problem and a technical one (Banks, 2021, p. 1052).

Thus, the technical component of attribution can be seen as a forensic, intensive process that can take significant time to be fruitful—especially if the attacker is 'sophisticated' (see Section 4.3) and has made clever skilful deceptive efforts to cover their tracks—and hence, even with 'next-generation research on attribution, technology can only be used to establish technical attribution' (Mueller et al., 2019, p. 113). It is still necessary to offer political or strategic-level attribution to make a more convincing prosecution of attribution, especially as it is possible to make it seem that cyber attacks have been launched by a third or innocent party. In other words, technical attribution is imperfect and is limited by the willingness of states to reveal the forensic

evidence they have collected over time. This then leads to public attribution being not only a technical decision but also a politically charged one that is perhaps based on probabilities and degrees of confidence, which are issues that will be expanded upon later in the chapter. Consequently, the technical challenges of public attribution will continue to strongly inform Australia's persistent stance of managing ambiguity in attributing cyber attacks, particularly when attributing as a standalone nation.

Thus, all the aforementioned caveats can potentially undermine or damage deterrence-by-denial and deterrence-by-punishment efforts, as the 'acceptable' timeframe for response could be shorter than the timeframe for any forensic investigation to produce explicit results and/or to identify and evaluate evidence that allows attribution (Libicki, 2009, p. 94).

Hence, while various attribution definitions do not differ greatly, the ongoing debate reflects the lack of consensus on what exactly attribution is from a legal perspective (Steffens, as cited in Janofsky, 2021). Regardless, there are some broad types of attribution. For example, there are multiple models, as discussed in the prior section. These models identify distinct levels of attribution, which are seen as technical and political or strategic. All these layers will combine to eventually form an attribution policy framework that aims to access an attacker's tactics and techniques as well as to be as accurate as possible about the origins of the attack—again, not only by using forensic evidence but also with a sensitivity to political realities in international relations (and the strategic ramifications of confronting China that decision-makers must consider prior to any publicly announced attribution).

4.3 How Sophisticated Are Cyber Attacks?

Cyber attacks can range from small to significant. Threat actors have rapidly increased in sophistication over the past year, using techniques that make them harder to spot and that threaten even the savviest targets. Nevertheless, one key problem is that if everything is deemed as 'sophisticated', then nothing is sophisticated in affecting security and defensive measures (Buchanan, 2017). Further, the term itself does not explain the spectrum of modern-day cyber challenges. States such as Australia also do not have a cogent, public list of cyber actions that explains the threshold between sophisticated and non-sophisticated. Ultimately, 'sophisticated' may indicate that an attack required some form of skill, but this is still a vague marker.

Thus, ultimately, sophistication is a contested term. Korzak & Guitton (2013) asserted that because of abstract ideas about sophistication, the label has potential for misuse, and it remains problematic when used to describe the practical technical considerations of cyber attacks, especially given how the threat landscape has evolved (p. 62). Further, the authors questioned how sophistication can be more clearly defined in order to better identify and defend against emerging exploits as well as influence wider policy debate. As Kleinman (2020) described, in almost 'every supposed 'sophisticated' attack, well-known and previously identified methods and vulnerabilities are the sources of exploitation'. Rarely do attackers construct from the ground up a completely bespoke cyber attack without using pre-existing tools (Bartos, 2016). The hacking or related job is simply made so much easier for an attacker if they use existing tools.

Rather, the literature has revealed a culture of poor risk management decisions and an aligned political uncertainty in defining what is and is not a 'sophisticated' cyber attack (Biscoe, 2018; Buchanan, 2017). Further, the word sophistication itself is also troubling as it represents a 'conventional wisdom' approach to deterrence and conflict, whereas the levels of actual sophistication in cyberwarfare are varied and numerous and there is a wide range of innovative threat actors (T McKenzie, 2017, p. 9). For example, a cyber attack can simply be related to poor cyber hygiene, such as weak passwords and unpatched systems. Thus, it has been argued that 'sophisticated' weapons are those precisely targeted at well-defended systems but with the trade-off of having a relatively short shelf life, that is, having single-use capability (Dortmans, Thakur, & Ween, 2015, p. 175).

Hence, a formal, consensual definition about what qualifies as a 'sophisticated' attack is lacking. However, as a starting point, it can be argued that sophisticated cyber weapons are those that are precise, have deliberate design in their impact and suit the discussion of strategic cyberwarfare as they are likely to be deployed against 'hardened' targets such as critical infrastructure sector assets (Libicki, 2009, p. 15). In terms of the delivery of sophisticated attacks at scale, it is also worth noting that the Australian Government's Critical Infrastructure Resilience Strategy in 2020 defined such critical infrastructure as

> those physical facilities, supply chains, information technologies, and communication networks, which if destroyed, degraded, or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect

> Australia's ability to conduct national defence and ensure national security. (as cited in Barbaschow, 2020).

Importantly, most cyber conflicts and data manipulation are not conducted with often-cited 'sophisticated' cyber weaponry, as these weapons are repeatedly 'target specific' and frequently have a short use-life because of their reliance on exploiting weaknesses in code and/or systems or personnel to be successful (Smeets, 2022). That is, as Buchanan (2017) stated, a wide variety of cyber operations

> are labelled as sophisticated because the definition is ambiguous. Too often, the metric for a so-called sophisticated operation is simply success. If the mission worked, it was sophisticated; if it failed, it was not. But this view is too narrow (p. 4).

The political ramification of labelling cyber attacks and related security incidents as 'sophisticated' is that the term can create unnecessary public anxiety. Moreover, such a label can blur the lines between what would justify more offensive retaliatory strategies versus counterespionage efforts or other low-key security related operations (Stone, 2013). In other words, there is a

> difference between a sophisticated threat actor and a sophisticated attack. The distinguishing factor is that the threat actor is better resourced for their mission. However, incident analysis provides evidence that most attacks utilize standard attack approaches simply because they work. (Kleinman, 2020)

This is understandable, for in the backdrop of any investigation that cannot identify or is unaware of a basic cybersecurity incident, the attackers could continue to exploit any design and implementation flaws. In short, motivated and smart attackers do not necessarily rely on 'sophisticated' methods.

As explained earlier, cyber attacks tend to rely on pre-existing weaknesses and security flaws in systems to facilitate the attacker's entry and exploitation of those systems. Hence, attribution and, in particular, the communication element of deterrence, will be affected, as states (or state-based actors) might potentially undermine confidence in intent and capabilities by falsely accusing actions as being more advanced or radical than they in fact are, perhaps to drum up domestic support or to add a perceived immediate diplomatic advantage when accusing a potential antagonist. The victim may even wish to create a smokescreen to deflect scrutiny from the primary cause of the successful attack, such as the failure to migrate an established

and existing vulnerability or shortcoming within their own IT system. The Optus breach discussed in Chapter 2 is a notable example of a relatively simple and opportunistic attack that the Optus chief executive officer tried to spin as sophisticated and an expert-driven unauthorised access (Palmada, 2022).

Thus, while some cyber attacks are certainly 'sophisticated', many others are relativity well known, standard and uncomplicated. At worst, overplaying claims about sophistication can make policy initiatives to defend against cyber attacks seem to be an exercise in either pointlessness or panic. This would also tie in to Libicki's (2009) question, 'Can we avoid escalation?'. Positioning policymakers to identify and label the nature of attacks accurately and honestly and to respond appropriately will remain an important dimension to attribution and how a state such as Australia may then construct a cogent deterrence framework. This would need to be a framework that will enable effective and timely detection, containment and, critically, a proportionate response. Such a framework will also be necessary to ensure that states aim to avoid poor cyber-hygiene practices and can distinguish between different types of attacks, including espionage as discussed in Chapter 1. As Smith stated, 'to date there has been an inability to acquire any substantial, irrefutable evidence of cyberwarfare, only speculations based on historical information, rumours, propaganda, and misinterpretation or misrepresentation of facts' (Smith, as cited in Shahid, 2020). Therefore, although cyber risks and the threats of aggressive cyber attacks are tangible, they can also become easily embellished with hyperbole and be expediently politically magnified.

This precise, honest public messaging (and any 'naming and shaming') will remain a needed component of a more tailored deterrence approach. In addition, a broader definition of cyber weapons might only include 'software and IT systems that, through ICT [information and communications technology] networks, manipulate, deny, disrupt, degrade or destroy targeted information systems or networks' (Uren et al., 2018). One lesson for policymakers would be to also distinguish between the 'sophistication' of incidents such as cyber espionage, offensive operations and other possible scenarios, including cybercrime and foreign interference.

4.4 Australian Context and the 'Name and Blame' Game

As stated above, attribution is when a specific actor is named as being responsible or accountable for a cyber anomaly or malicious act, for example, the theft of data from a computer network (Levite & Lee, 2022). Multiple actors can be on the receiving end of such

public attribution, ranging from specific nation-state governments to criminal networks and transnational state-backed hackers.

Therefore, conducting investigations and the requirement that the attribution should be accurate—albeit perhaps not necessarily proving 'beyond a reasonable doubt' in strict legal terms—that can determine who has attacked a system in a specific period remain both problematic and contested in efforts by the Australian Government to produce 'confident' attribution and deliberate and targeted countermeasures. In short, properly attributing a cyber attack 'is a recognized difficult problem owing to both the technical acumen required to conduct forensic analysis and the ease in which an attacker can deliberately obscure its identity' (Welburn, Grana, & Schwindt, 2023). Hence, Australia might be well placed to deter attacks, albeit with imperfect attribution. Furthermore, it may be that the threshold for 'reasonable' evidence lies in the political judgements of Australian decision-makers as well as in consultation with Australia's allies, especially if used to justify retributive counterattacks. A critical consideration for Australia will always be escalation and ensuring that malicious activity stays in the cyber domain, meaning offensive operations must be considered extremely carefully, particularly if deployed against China.

Nonetheless, in a strategic sense, Brenner (2007) asserted that attribution essentially encompasses two central issues, that is, identifying the attacker and determining the type of attack. Accordingly, the context for cyber attribution that informs cyber deterrence is that attribution posits the requirement of laying blame on an actor for committing an action that is then interpreted by Australia as an attack with various disruptions and costs. This presents Australian policymakers with many key challenges. They must be able to assert what is an aggressive and deliberate attack, be confident that they have attributed an attack that crosses an unacceptable political threshold in terms of a disruptive or even destructive effect and, ideally, be prepared to signal or assert attribution either publicly or, as Libicki (2009) argued, through *sub rosa* communications (pp. 99, 117). Libicki even suggested that a general population may be totally uninformed or unsuspecting of events occurring at a diplomatic level or in regard to offshore activities. This is supported by comments from ASD Director Rachel Noble confirming that there are '10's' of retributive actions undertaken by ASD against foreign targets (Crozier, 2023). If thresholds are not explicit, then by a consistent course of actions and public admission of said actions Australia could send China a signal about unacceptable thresholds.

Further, while it may be possible to assert through attribution from which country an attack had originated, challenges arise not only in ascribing guilt with absolute certainty but also in defining the aggressor's precise motivations and intent. This makes it difficult to prove that the motivation of an attack was actually conceived primarily as a goal of a state-based attack as opposed to, for example, a rogue actor or other non-state entity, which also will typically require a high level of forensic evidence to support the attribution (Maglaras et al., 2019). Further, no international convention governs state-based cyber attacks in the way, for instance, that the Geneva Conventions cover the rules of warfare, and thus, there is no straightforward conventional legal method or law enforcement process—or method to best place pressure on the accused attacker—that is wholly accepted by the international community (Mueller et al., 2019, p. 108).

As a result, cyber-attack attribution remains a complicated task. Understanding the elements of an attack environment is also clouded by a game of possible motivations from criminal to political to personal. Attackers will generally try to hide both their identity and location. Therefore, in attempting to identify the culprit and their motives for the targeted cyber attacks, attribution is tied to a multi-tiered deterrence approach. Again, Libicki (2009) described deterrence options as deterrence by denial (the ability to frustrate the attacks) or passive deterrence, and deterrence by punishment (the threat of retaliation) or active deterrence (p. 27). These deterrence concepts can also be referred to as 'deterrence in kind', to demonstrate that the type of deterrent mechanisms being examined remain within the cyber domain and are attached to non-kinetic warfare strategies. It is also worth reinforcing that although attackers or adversaries will complicate attributions by deliberately obscuring identities, the associated aim to 'know one's enemy' can also be invaluable for political and strategic aims relevant to the clarity and credibility of punishment itself. In other words, attribution will directly feed into risk management opinions to assist assessment purposes and might then offer valuable intelligence and related insights to direct an effective and proportionate response (Coppell & Chang, 2020).

In this regard, Rid and Buchanan (2014) encapsulated some of both the nuance and the distinctiveness of cyber attribution in stating that 'attribution is an art: no purely technical routine, simple or complex, can formalise, calculate, quantify, or fully automate attribution' (p. 30). Significantly, from a perspective of politics and diplomacy, the more technical challenges of attribution 'depend on critical organizational and political context that is making attribution,

and thus deterrence, harder and easier alongside different dimensions' (Lindsay, 2015, p. 54). In other words, the call for public attribution will remain a policy matter that is heavily tied to the considered political choices and strategic context. In short, open information dissemination about the nature and origins of a cyber anomaly should be a calculated cost–benefit process of political decision-making—and in the case of China, any action must be taken after considering the impact of real or perceived provocation.

For instance, in July 2021, Australia, in consultation with its allied partners, directly accused China of exploiting vulnerabilities in Microsoft Exchange software to negatively affect computers and networks globally, including in Australia itself (M Payne et al., 2021). Former Home Affairs Minister Karen Andrews stated that evidence had been found that substantial Chinese Government-sponsored attacks were part of a reckless but familiar pattern of behaviour that 'opened the door for cybercriminals to exploit (Australia's) private sector for illicit gain' (M Payne et al., 2021). Indeed, having multiple Australian ministers publicly call out these specific cyber attacks as international law violations in a joint address was a significant step forward in approaches to attribution and signalling to shape behaviour. Further, it illustrated a growing level of confidence that entities such as the ASD were able to provide evidence to guide cyber attribution as well as the political calculation to demand accountability in cyberspace in the public sphere. Furthermore, the 2021 comments that assigned a particular malicious act to China were also important for reinforcing the value of public–private partnerships in the cyber domain, including the value of the commercial sector to better protect infrastructure assets via deterrence by denial (Temple-Raston, 2021).

Indeed, as Xu Manshu (2022) asserted, cyber attacks have flourished in recent years to incorporate commercial tools in efforts to help mitigate the defences of public and private assets:

> Advanced persistent threat actors are increasingly making use of widely available commercial tools such as virtual private networks. Many organizations provide ransomware services, with core developers maintaining ransomware and payment sites and recruiting affiliates carrying out attacks and disrupting victim networks. In return, any ransoms paid by victims are split between core groups and affiliates, which typically receive 70–80 percent of the total (p. 26).

Consequently, adding to the debate surrounding cybersecurity and attribution is a burgeoning industry in which Chinese APTs are being deliberate in their choice of corporate and private

‘victims’, often regardless of wider political or diplomatic tensions about the economic espionage aspects of the cyber domain. Chinese espionage operations have ramped up at such prodigious scale and pace that some commentators have asserted that ‘the Chinese have more data [about ourselves] than we have on ourselves’ (Evanina, as cited in Temple-Raston, 2021). In this example, the quotation refers to the US, but it is emblematic of the scale of activity being undertaken by Chinese APTs.

Certainly, in many other similar cases, former Australian Governments stopped short of publicly and formally attributing blame to a particular actor such as China (Packham, 2019). Nevertheless, on this occasion in the backdrop on the 2021 incident, Karen Andrews and others stated that

> the attribution had been part of “a global response” and not just “Australia on its own. …They (China) have been called out and we will continue to call out, not only China, but other nations, if they do launch and undertake significant attacks here on Australians and Australian businesses”. (Hurst, 2021)

Consequently, the above signalling of the ‘the rules of the game’ highlighted that public attribution will, and does, remain a political choice beyond the application of technical capabilities. For Australia, the 2021 step to publicly attribute cyber incidents to a specific state is especially noteworthy, given that the former Morrison Government had also been routinely accused of being ‘soft’ in not explicitly categorising the Chinese as responsible for other incidents in which they had exploited Australian cyber vulnerabilities. Prime Minister Morrisson had sometimes opted for open-ended political language instead, such as a ‘sophisticated state-based actor’ (Hurst, 2020). Furthermore, the new Cyber Incident Management Arrangements via the ACSC would aim to initially mitigate the impact of any national-level cyber incident and then might declare a national cyber incident in support of, and consultation with, relevant cross-jurisdictional actors. The Cyber Incident Management Arrangements ‘outlines the inter-jurisdictional coordination arrangements, roles and responsibilities, and principles for Australia government’s cooperation in response to national cyber incidents’ (ACSC, 2023), essentially functioning as a part of the executive-level management for national cyber incidents.

However, even during any national cyber incident, public attributions of malicious activity remain squarely political actions. In 2021, Alastair MacGibbon, the former head of ACSC even noted

> it's not been common for Australia to attribute malicious cyber activities to China so it should be treated as serious when it does occur. This was a particularly reckless series of acts by China and its contractors who, according to the allegation, have carried out criminal acts at the same time. (Galloway, 2021).

It can also be argued that the 2021 assessment revealed that deterrence-by-punishment frameworks were not satisfying the Australian Government's security and stress-testing needs. However, the flipside for the government was that overreacting without prudent communication might cause an escalation with China, which is also a failure of deterrence, as the signalling strategy should not promote further conflict and any cost–benefit initiatives should be judged as efforts to reduce, rather than increase, the chances of extended cyber conflict.

Therefore, the former Morrison Government in 2021 appeared to have calculated that the public attribution of China would serve a signalling function that, in turn, would not exacerbate the risk of inadvertent political escalation, despite the CCP's public condemnation and threats (Saukonoko, 2021). As mentioned, it also indicated that the government had the technical capability to deal with the attribution problem—a problem spotted and shared within allied global networks and addressed with a coordinated disclosure. Such developments and their potential consequences in dealing with issues such as cyber espionage had been formally alluded to in official policy in 2020. As stated in the 2020 Cyber Security Strategy, Australia will 'respond to malicious cyber activity directed against our national interests. We deny and deter, while balancing the risk of escalation. … We can choose not to respond' (Department of Home Affairs, 2020, p. 26).

Interestingly, a prior report commissioned by the Australian Government to help to inform the design and direction of the 2020 Cyber Security Strategy had urged policymakers to more habitually 'name and shame' countries that launched large-scale, disruptive cyber attacks (Galloway, 2020). The advisory panel argued that there was an urgent need for there to be 'clear consequences' for nation-states (and cybercriminals) and had recommended an increase in the frequency of the direct attribution of state-based cyber attacks 'where necessary and appropriate' (Galloway, 2020). Former Assistant Defence Minister Andrew Hastie later added that the fact that multiple like-minded nations such as Australia (and mainly other US allies) had joined together and pinpointed China for cyber attacks in 2021 was a very 'sound development' (Hastie, 2021).

Further, it could be inferred that by incorporating related clusters such as cyber hackers and state-sponsored criminals, the Australian Government was hoping to give itself some mobility to increase the effectiveness of political signalling against shifting targets. Questions of anonymity and attribution would remain linked to the interconnected and nebulous nature of the cyber domain, despite the Chinese Government's habitual reference to random 'patriot hackers' as the core cause of these types of cyber intrusions, the inference being that it had not endorsed or directed the actions (East, 2022; Laskai, 2017).

Certainly, allied actors, including the US, have sometimes responded by publicly asserting that various cyber groups appear to have significant crossover between state and non-state entities (Blinken, 2021). The implication is that states such as the US and Australia might be less reluctant to circulate information about the cyber intrusions than they had been in the past, while policy framing would shift from reactive towards more active deterrence strategies, such as the issuing of arrest warrants for foreign cybercriminals or even directly accusing the Chinese Government of not doing enough to control or mitigate the actions of malicious cyber actors inside its own borders (Lyngaas, 2018).

Significantly, the former Morrison Government did not explicitly answer why it had chosen to suddenly adopt the concept of public signalling in regard to China in 2021. Nonetheless, at the very least, it did appear that Australia and its allies such as the US were seeking a common language and signalling framework to put forward a shared, more consistent cyber approach to deterrence strategy and to set clear expectations on accepted behaviour based on cost–benefit calculations, despite individual variations on what 'red lines' in cyberspace might actually entail. Indeed, since 2019, the AUS-US Cyber Dialogue has aimed to provide a better calibrated strategic direction through the combined development of cyber capabilities. Further, the Fifth India-Australia Cyber Policy Dialogue was held in 2022, further cementing the relationship between the two states (Department of Foreign Affairs and Trade, 2022). The attendees for this dialogue included senior officials from India's National Security Council Secretariat, the Ministry of Home Affairs and various technology and critical infrastructure departments, signalling the extended collusion between security and infrastructure for the two countries. In 2023, the Albanese Government reinforced the importance of 'working in partnership with our Pacific neighbours to lift cyber-security and build a cyber-resilient region' (O'Neill, 2022).

Overall, the option of 'naming and shaming' actors such as China in the cyber domain can be seen as a deliberate component of a cyber-deterrence strategy, especially if used to justify

reactive or offensive policy response actions. Any state (or collection of states) that points the finger to states engaging in or sponsoring cyber aggression will need such attribution claims to be credible, honest and as accurate as possible. Thus, while not necessarily terminating all malicious cyber activities, publicly naming cyber attributions does

> impose costs and send important signals, even when not accompanied with sanctions or other punitive measures. … Put plainly, states do not like to be called out. It isn't surprising that cyber attributions are often met with loud rejection, denial and condemnation. Importantly, when such attributions are accompanied by evidence and explanation based on skilled forensic investigation, they demonstrate a capability to discover who's responsible for malicious behaviour, down to the level of units and individuals (Carvin, 2021).

In short, making attribution information public, as done in 2021, signals both intentions and capabilities. It is an explicit gesture to targeted actors such as China that hacking and other cyber mischief can and will be discovered, and then, the threat of retaliation will be considered valid via diplomatic (or other) routes that align with Australia's international allied engagements.

4.5 Caveats

Of course, such 'name and shame' actions are also not without potential downsides and shortcomings. No state wants to become 'the boy who cried wolf' and add to instability in cyberspace and escalation (Carvin, 2021). After all, deterrence is a mitigating effort to establish a reasonable set of expectations that aims to encourage potential attackers and adversaries to believe it is not in their best interest to attack. At the very least, it involves a psychological component and should be designed to help shape and limit the overall frequency and severity of cyber anomalies and associated malicious activity.

In efforts to influence the risk-taking propensities of actors including China, situational awareness is another key factor. As Libicki (2009) argued, states that reveal attackers but do not exert time-sensitive pressure or intimidation can de-legitimise deterrence theory or even grant the original attacker too much time to assume an expectation of impunity (pp. 93–94). However, cyber attributions could arguably be most effective when reserved for only the most serious 'watch-and-warning' attacks. Libicki (2009) also argued that publicly revealing an attack offers the opportunity for not only public 'name and shame' but also conducting *sub rosa* responses to influence an adversary's decision-making calculus (p. 92). By this reasoning,

then Prime Minister Morrison might have openly announced knowledge of cyber attacks from China in order to pre-empt and mitigate the CCP's outrage over the reciprocal employment of Australia's cyber-offensive capabilities in retaliatory attacks on China's own information networks.

Of course, any retaliatory policy options are not necessarily purely cyber but can be multifaceted and include political options and diplomatic actions. Moreover, not all types of cyber attacks will merit the same kind of policy response, since some maliciously deploy code to destroy or degrade critical infrastructure, whereas others such as the aforementioned Microsoft Exchange attack pilfer information from email servers. Therefore, to be effective at cyber deterrence, policymakers will need to discern the purpose of a cyber attack. As stated earlier in this thesis, strategic cyberwarfare is a campaign of cyber attacks launched against a state and society to affect the target state's behaviour and differs from more conventional forms of strategic coercion (Libicki, 2009, p. 117). Accordingly, attributions of these campaigns and responses against a state will be varied and should be tailored. As a starting point, investigating the desired deterrence effects on adversary conduct, determining the resources and skill sets required for attribution to pinpoint attacks, deciding on the policy tools to be employed to achieve desired outcomes and examining the wider strategic context will all be crucial to understanding attribution frameworks, the types of costs and punitive measures that might be effective and overlapping cost–benefit policy calculations.

In the backdrop of the development of capacities to respond flexibly and effectively, Australia's 2020 Cyber Security Strategy explicitly declared that the Australian Government would continue to build strong cyber defences and to 'publicly call out countries when it is in our interest to do so' (Department of Home Affairs, 2020, p. 26). Peter Jennings, a former senior defence official, also argued that past Australian Governments had too often raised the matter of cybersecurity without sending strong, credible deterrence signals to influence perceptions and motives, such as the failure to openly name the chief suspect, China, in efforts to indirectly encourage more responsible behaviour (Hurst, 2020).

Hence, given the inherent challenges of attribution (and deterrence objectives in a strategic context), the consequences of misattribution and the logic of cyber-crisis management must always be considered, especially in light of Libicki's (2009) key questions:

1. Do we know who did it?

2. Will third parties join the fight?
3. Does retaliation send the right message to our own side?
4. Can we avoid escalation?

Significantly, the importance of such open-ended questions has increased since *Cyberdeterrence and Cyberwar's* publication in 2009 owing to their immediate correlation with attribution, the absence of formal international arrangements to direct cyber behaviour and the ongoing ramifications of factors such as the risk of misattribution in cyberspace. For example, 'deliberate misdirection of an attack's source muddies the waters, causing victims to waste valuable time and resources on trying to assign the blame rather than focusing on the immediate responses needed to prevent further harm' (J Thompson, 2020). Consequently, without applying a tailored deterrence strategy and clear methods to publicly disseminate evidence with confidence, attribution will be challenging in efforts aimed at effective deterrence by punishment and related policy deliberations, which is the focus of Chapter 5.

It is worth highlighting that unlike a missile attack or other kinetic attack in the physical domain, a cyber attack can often leave sparse initial evidence behind for the defender to immediately determine who attacked. In fact, Australia may have the 'right' pieces of evidence but interpret the evidence incorrectly or may be incapable of understanding the evidence in pursuing its cybersecurity objective (Rid & Buchanan, 2015). Thus, retaliating without a fundamental understanding of 'do we know who did it' could be highly counterproductive, provocative and dangerous in creating new or antagonising 'enemies'. At the very least, an 'acceptable' level of attribution must be performed prior to the commencement of any retaliatory action. Such a calculation does appear, on the basis of the 2021 incident, to be a combined and collective technical and political decision. Of course, in attribution, Australia might may also wish to convince other third parties, whether international observers or its allies, that the attribution is accurate and demands a proportionate response that will not have a counterproductive cascading effect (Hare, 2012). Thus, a mix of political, strategic and evidence-based technical analysis in Australia seems to have set a threshold for 'acceptable' attribution.

Last, in addressing future attribution challenges for Australia, some level of secrecy in relation to specific deterrence goals or even offensive retaliatory capabilities might still conceivably remain. The development of better technical attribution capabilities will still be balanced by the need to preserve alliance cohesion and political de-escalation in the context of extended

deterrence coverage. For example, if sensitive forensic techniques are too openly disclosed, policy responses may backfire or such information may merely inform the attacker about ways to better hide or integrate future attacks (Libicki, 2009, pp. 49–50).

4.6 Attribution Models and Deterrence in the Cyber Era

Attribution, both political and technical, is a high-priority deterrence goal. As stated, carefully unpacking attribution is important for any deterrence strategy and Libicki's framework, not only for determining 'do we know who did it' but also for answering three related questions: 5: Will third parties join the fight?; 6: Does retaliation send the right message to our own side?; and 8: Can we avoid escalation? Rather than getting bogged down in technical details about some of the available methodologies utilised by various actors to investigate attribution, this section aims to construct an extended picture of the actions involved in attribution in the establishment of a cyber-deterrence strategy, to add to the analysis of the Australia–China case study through Libicki's framework of deterrence by punishment.

In developing metrics for attribution and assessment, different entities and actors have constructed models of attribution to send credible cyber-deterrence signals through collected evidence/intelligence, which is partially an investigative design that compares activity to previously known tactics, techniques and procedures of threat actors such as China (see Mueller et al., 2019). These tactics, techniques and procedures are built by analysing past incidents to identify the intrusion sets or the tool set deployed during cyber-attack patterns that are then grouped together and associated with a common actor in any deterrence calculus (Mueller et al., p. 109).

Attribution models used to ascertain ways to influence adversaries and to react accordingly, include the Q model from Rid and Buchanan (2015) and the diamond model of intrusion analysis from Caltagirone, Pendergrast and Betz (2013). There is also Lin's (2016) model which uses three levels of attribution, focusing attribution on machines, human operators and ultimately the responsible actor (p. 3). This model has some public fame as the model deployed by Mandiant in the attribution of the infamous Unit 61398—APT-1—tied to the PLA (Mueller et al., 2019).

Further, the Lin (2016) model has certain strengths in identifying the specific IP address of the computer as a first step, then the user and then the entity responsible for significant cyber

attacks (p. 14). Conversely, the Q model is also described as a 'function of what is at stake politically' (Rid & Buchanan, 2015, p. 7). Thus, the motivations and likelihood of an attacker going through the difficulty of conducting a strategic cyberwarfare attack is strongly considered in the Q model. These examples are presented here to illustrate the existing methods of attribution. However, it is unclear whether entities such as the ASD use one or either of them, whether the ASD uses any publicly available attribution models and whether the ASD even has a systematised approach to attribution. Since this knowledge is lacking, these models are instead described to provide concrete examples of attribution in academic literature and confirm that methodologies are available whose application *can* strengthen deterrence efforts.

Given the desirability of deterring cyber attacks by the ASD, it can be argued that a multi-method framework will often determine the initial 'who did it' analysis. Instruments such as atomic, behavioural and computed can all provide a framework that analysts can utilise in efforts to determine breaches and attacks. For instance, an atomic indicator is a piece of data that cannot be broken down or reduced without losing its forensic value; effectively, it is already 'atomised' and cannot become any smaller without becoming problematic for credible analysis. Some examples include IP and email addresses, small pieces of text and items such as domain names (Ramsdale, Shiaeles, & Kolokotronis, 2020).

Next, computed indicators are those which are derived from data in an incident (Hutchins, Cloppert & Amin 2011). Computed indicators could be a 'hash', which is a unique signature derived from input data. Therefore, hash values change according to inputs—if the input does not change (e.g. the password), neither does the hash. Last, a behavioural indicator is a combination of action and other indicators, such as the actor attempting to clear system event logs to hide the activity of an intrusion, and therefore, the action may contain more evidence than just of a technical nature. In short, certain actors such as China may be attributed certain actions or 'styles' and detection signatures.

Thus, entities such as the ASD that carefully and routinely defend their networks and other networks in Australia can utilise these attribution methods as a form of hunting guidance. Once they find evidence or an indicator of a compromised system or network, associated entities can unpack further technical questions and can launch the attribution process and overlapping cyber-deterrence methodologies and metrics in order to aid the ASD in hunting for this activity. Significantly, the order of such indicators can vary or might even be legitimate system

commands (Rid & Buchanan, 2014). Consequently, care should always be taken not to automatically assume that such findings indicate malicious activity.

All these approaches acknowledge the necessity of the non-technical dimension to attribution, which Mueller et al. (2019) argued as a necessity 'to hold offensive actors responsible for future cyber-attacks' (p. 107). Furthermore, when states are engaged in developing attribution models founded on inter-agency cooperation and collaboration, such as that between ASD and the Five Eyes, it can lead to a more time-sensitive, resource-efficient cyber-deterrence policy (Lynch & Morrison, 2023).

Accordingly, technical and non-technical dimensions to attribution will both continue remain central for Australia. Again, Rid and Buchanan (2015) have provided a highly constructive definition of attribution, asserting that attribution is what states make of it, given that attribution is 'an art as well as a science' (p. 7). Moreover, in strategic terms, attribution will remain a function of 'what is at stake' politically, while technical attribution is a nuanced process in matching a cyber assault to an offender while recognising the limitations or challenges of accuracy in order to reduce the risk of mistaken identity. Therefore, there is a sliding scale of attribution from a broad-based attribution, which could function in geographical terms (i.e. stating it was a Chinese cyber attack), to a more fine-tuned forensic attribution (e.g. the tracking by private entities of APT Putter Panda to the streets of Shanghai as far back as 2014; see CrowdStrike Global Intelligence Team, 2014, p. 5).

In this sense, establishing attribution for cyber operations in Australia will remain multifaceted and complicated although not unattainable or impossible (Janofsky, 2021). In other words, attribution will remain a complex process that often tends not to offer simple and necessarily immediate results, but instead elevates 'shades of grey' based on particular circumstances. Given that attribution is part of a function of what is at stake politically, any technical inquiry will always be intermingled with the ideology, domestic context and political instincts or inclinations of key decision-makers in Australia and elsewhere (Hare, 2012; Skopik & Pahi, 2020).

One international example of the role of political considerations in shaping and determining national responses, which will work in tandem with the strength of the forensic logic linking the evidence, was in 2010. Despite no state actor being formally accused of implementing the Stuxnet attack on Iran, the cyber attack was widely attributed to Israel and the US by Iranian

officials via media reports (*Iran Builds Firewall Against Stuxnet*, 2019). Iran also made some other cyber-sabotage accusations in the media, but these were also not followed up on in any official way or were seen as triggering a deliberate and counter-retaliatory cyber attack against Israel and the US (Abdollah, 2019). It appeared that Iran policymakers did contemplate that an official public shaming might result in a highly disruptive and escalated political and diplomatic international dispute. Nonetheless, it is worth noting that in 2020 Iran eventually stated that it would retaliate against 'any country' that carried out cyber attacks on its nuclear sites in the backdrop of fire at its nuclear Natanz plant—a fire that some Iranian officials again stated may have been caused by cyber sabotage (*Iran Threatens Retaliation*, 2020).

A similar situation arose for Australia, as mentioned, which despite suffering significant cyber attacks, including on both major political parties' websites before the federal election in 2019, was still unwilling to publicly attribute the attack to a specific actor and, rather, merely acknowledges that it occurred (Packham, 2019). This had generally been the case when Australia was the victim of other similar offensive cyber operations, which had resulted in a consistent avoidance and hesitation to 'name and shame' (Bushell-Emblind, 2020).

Yet, as stated, this positioning appears to have changed, as with the support of the US and others, the Australian Government has indicated a willingness to openly identify the aggressor, namely China. Indeed, in 2021, the Australian Government was again among the first of many international entities, including NATO, in declaring that China was responsible for exploiting a vulnerability in Microsoft Exchange mail servers that had far-reaching negative implications globally (J Evans, 2021). This is particularly important as the then Home Affairs Minister Karen Andrews plainly stated that this revised policy position would continue into the future: Australia had now taken the official attitude of publicly attributing at least some (undisclosed) threshold of malicious cyber actions to the Chinese (Galloway, 2021). As was also detailed in Chapter 2, the Minister's comments about the revised policy position not only held true but also continued despite a change in government in 2022. Importantly, this attribution case did implicated not only China but also its MSS specifically, which, as detailed in earlier chapters acts as China's offensive cyber-operational entity, which again pointed to high-level ASD capability (Hurst, 2021).

4.7 Legitimacy and Why Is Attribution Significant for Policymakers?

Yet, such capacity development and related tools studied in isolation are incomplete, for decision-makers will still require deterrence planning and political clarity in responding to incidents as Libicki's framework stipulates through questions such as '*Do we know who did it?*'. As stated, attribution is a deterrence starting point that helps decision-makers identify required capabilities and ensure that they do not escalate the matter by a disproportionate response or inadvertently accuse an uninvolved actor. It could also tell decision-makers whether they should even care about this cyber incident in the first place. Attribution also allows Australia to respond to aggressive cyber actions because it not only answers who attacked Australia but also how, and therefore what responses Australia might deploy that will remain appropriate and proportional.

The ACSC has also increasingly collaborated with both the private and public sectors to share information on threats, increase resilience and improve coordination for responding to cyber attacks. This approach has involved a general cyber-deterrence model that has allowed the integration of public–private techniques to increase awareness of cybersecurity risks and allow an extended collaboration to assist a more layered, 'active' defence that can involve the defence and intelligence sector (Janofsky, 2021). For example, Australian intelligence and military leaders 'have begun to look beyond reactive, tactical cyber defence to the formulation of a proactive, strategic cyber-defence policy, which may include international military deterrence' (Geers, 2010, p. 299).

Further, rather than a reactive strategy, such connectivity can also encourage mitigation-based planning and elevates public awareness to various cyber activities. Thus, correct attribution will continue to provide a drive for closer collaboration with relevant partners as well a general diplomatic and political purpose that can facilitate decision-making, including about whether policymakers should (and to what extent) carry out retributive and punishment actions either alone or with the assistance of allies (Bassi, 2023).

For instance, as the precise 'battlespace' in the grey zone grows more difficult to define, if the political leadership discovers that Australia has faced a cyber attacked by the Chinese (either through public or private entities), then the Australian Government could potentially seek allied assistance in any 'name and shame' policy to then determine and justify the nature and type of any punitive actions in response. Further, if this course of policy action is publicly announced,

decision-makers would need a range of political, diplomatic and military options to support their cost–benefit calculations and to ensure a legitimate, credible response:

> If the target does not follow up its claim of an attack with an attribution, it raises the difficult 'why not' question and encourages free lancers to make up their own minds on the matter (and perhaps take independent action). (Libicki, 2009 p. 93)

Thus, the process of assessing attributable attackers and the source (or backer) of any malicious cyber activity is important for threat assessments and for giving legitimacy and projection to any policy measures that Australia and others may undertake in response. This process will at least indicate Australia's technical capacity and provide the Australian public a level of confidence in the disclosed cyber assessment and an affordable counterstrategy. Given the diversity of potential adversaries, public attribution will give the impression of legitimacy and a broader political and strategic agenda, much like when the then Prime Minister Morrison had announced a significant breach by a 'sophisticated state-based actor' that was later identified as China in its conducting of attacks on critical infrastructure (Packham, 2019).

In such circumstances, the Australian Government requires precise guidelines or clear thresholds to justify potentially intrusive efforts to attribute cyber attacks on certain Australian networks. As Barbaschow (2021) stated:

> Before stepping in, the government must be satisfied that a cybersecurity incident has occurred, is occurring, or is imminent; that the incident is having a relevant adverse impact on the functioning of a critical infrastructure asset; the incident is posing a material risk to the social or economic stability of Australia, its people, national defence, or national security; the relevant entity or entities are unwilling or unable to take all reasonable steps to respond to the incident; and no other options for a practical and effective response exist.

This does not clarify exactly what Australia would consider a threshold and, instead, leans on what was stated earlier about effects rather than specifics: Australia does not tolerate adverse effects on critical infrastructure, but leaves the definition of adverse effects to the decision-maker at the time instead. This type of threshold aligns with Libicki's (2009) definition of strategic cyberwarfare in that it is a sustained campaign against an entity or entities in order to affect the decision-making capabilities of the state itself (p. 117). While such actions might add an extra layer of capability to Australian enterprises, imposing such 'red lines' is also important to dissuade and deter potential attackers. In contrast, to place thresholds impractically so that

they may never be crossed might also undermine options for responsiveness and the deterrent value of these initiatives. The quotation from Barbaschow (2021) does indicate a quite high threshold. Hence, in such instances, a (Chinese) attacker might decide to use a lower-level entry vector such as phishing attacks to not only enter targeted networks but also avoid the putative and disruptive retaliation that would be caused by their crossing a 'red line'.

In addition, the ambiguity often involved in attributing the source of an attack can complicate such deterrence models (and undermine national situational awareness) in various ways. As mentioned, deterrence itself can be captured within, and is reliant on, two core functions: technical capability and political calculation or resolution (Stone, 2012). Hence, although attribution remains part of technical capability, it will continue to be shaped by political cost–benefit calculations and can play a part in strengthening policy incentives to communicate 'unacceptable' damage. Libicki (2009) added that such components of deterrence in the cyber domain should largely take place formally between, and determined by, state actors. Therefore, despite any significant increase in the capability of the private sector, ASD assistance or associated policy measures, including offensive cyber operations, should then remain the remit and prerogative of the incumbent government, which remains best placed to implement a tailored deterrence framework.

In summary, official and public signalling to actors such as China that the Australian Government is aware of malicious activity will remain an important facet of a deterrence architecture that is fundamentally built upon the production of successful attribution. Correct attribution provides validity and credibility to all levels of the state apparatus in direct or indirect communications with foreign actors. Concurrently, improvements in attribution that strengthen deterrence can provide reassurance to Australian stakeholders about the ASD's competency while signalling that, at the very least, Australia is more than technically capable of attribution and therefore of defending its networks.

In this regard, Libicki's (2009) framework itself strongly emphasises deterrence by punishment as part of this strategic calculus. As aforementioned, the stated aim of deterrence is predominately to create disincentives for starting or carrying out hostile actions. In this sense, it is similar to nuclear deterrence in which the parties are 'mutually assured' that there will be at least an 'equal' and an opposite reaction. Thus, in search for proportionate, cost-effective solutions,

> if deterrence is to work before the first retaliation takes place, others must have confidence that the deterring state will know who attacked it. Hitting the wrong person back not only weakens the logic of deterrence (if innocence does not matter, why be innocent?) but arguably makes a new enemy. … The defender must not only convince itself but should also convince third parties that the attribution is correct (Libicki, 2009, p. 41).

Of course, and alternatively, without accurate and credible attribution, Libicki's (2009) framework of deterrence becomes significantly problematic, and many of the policy questions posed about deterrence posture and appropriate responses become very difficult to answer for any extended cyber-deterrence coverage. Consequently, attribution is fundamental to assuring both domestic and foreign actors about the accurate origin and source of any cyber attack in order to then justify and direct a proportionate, effective policy response.

4.8 Australia's Capacity and Attribution Examples

Australia will continue to try to manage consistent and numerous small and large-scale cyber campaigns carried out by actors such as China. A central challenge is to build and ensure rapid and robust attribution capabilities to assist in deterrence efforts and to signal unacceptable behaviour in cyberspace. In 2021, the Australian Government announced that cybersecurity was the 'number one' priority for the Home Affairs Minister (Andrews, 2021). In reviewing the Australia–China relationship as a case study, areas such as capability/technical expertise and political judgement will all continue to play a role in the relative strengths and weaknesses of cyberwarfare and related attribution challenges.

In this context, Australia's attribution capabilities should be assessed against Chinese cyberwarfare capabilities. As stipulated at the beginning of Chapter 2, therefore, any Australian national security approach to deterrence will need to comprise an understanding of the logic and capabilities of other cyber actors and rival states. As already mentioned, the attribution process has many features, from the technical collection of evidence and investigations about whether the cyber activity could be expected to cause serious damage, to political or strategic prosecution of this evidence, either via *sub rosa* responses, legal proceedings or specific 'naming and shaming' as Australia did against China in 2021 (M Payne et al., 2021; Rid & Buchanan, 2015, p. 4). Analysing and assessing Australia's attribution capabilities will require careful consideration of all these points.

Australia has also stated that it wishes to support global responsibility and enhance its influence in cyberspace. Overall, in the context of deterrence, having an effective capability could translate to self-defence and 'possessing the resources, skills, knowledge, operational concepts and procedures to be able to have an effect in cyberspace. In general, capabilities are the building blocks that can be employed in operations to achieve some desired objective' (Uren 2018).

For example, the government launched a range of cyber initiatives in 2022, such as REDSPICE, as discussed in Chapter 2 (Winkler, 2022). The stated aim was to enhance both the offensive and defensive cyber (and intelligence) capabilities of the ASD and focus on building resilience in the critical capabilities of the ASD's operations. Such ASD expertise can serve as a useful demonstration of Australian cyber capabilities and the ACSC, which operates within the ASD, also acts as a useful signalling demonstration of attribution capabilities, including numerous campaigns in which the ACSC has been involved that have demonstrated built-in resilience, global cyber cooperation and the robust attribution of malicious cyber operations that are publicly releasable.

4.8.1 Living Off the Land to Avoid Detection

The ACSC has crafted and supported a deterrence strategy with multiple response options, countermeasures and related attribution campaigns.

For example, in May 2023, an advisory statement from the ACSC and Australia's Five Eyes partners highlighted 'a recently discovered cluster of activities of interest associated with the People's Republic of China (PRC) state-sponsored cyber actor, also known as Volt Typhoon' (Australian Signals Directorate, 2023a). This Chinese-backed hacking group had aimed to commit espionage and gather information on the US and allied critical infrastructure and military capabilities. The advisory statement indirectly noted that Chinese tradecraft has improved and also publicly detailed how Volt Typhoon conducted 'stealthy and targeted malicious activity focused on post-compromise credential access and network system discovery aimed at critical infrastructure' (Australian Signals Directorate, 2023; also see Microsoft Threat Intelligence, 2023).

Hence, while China probes critical infrastructure in this manner frequently, such efforts to gain unauthorised access to systems have also exposed and displayed how tradecraft advancements have shifted over a period (Microsoft Threat Intelligence, 2023). The advisories detailed that

Volt Typhoon deployed highly technical skills whereby the attackers leveraged existing software on the target systems (Cyber Security and Infrastructure Security Agency, 2023). This act is termed ‘living off the land’ since it enhances attackers’ stealth capabilities as they need not conduct activity that generates ‘noise’, such as installing unique software that may face problems owing to the cyber defences installed on the targeted network.

Interestingly, the ASD (2023a) advisory in May 2023 stated that China has APTs that can conduct espionage, and potentially cyberwarfare activities, by circumventing ‘end-point detection and response’ technologies, which typically detect an attacker moving data from their own host network to the victim. The insinuation here is that Volt Typhoon has the capability to overcome or sidestep deterrence-by-denial policy frameworks.

Therefore, even if the defender can only ‘imperfectly’ attribute attacks, such tradecraft by China again demonstrates the importance of establishing tailored ‘naming and shaming’ parameters and also allowing scope for deterrence-by-punishment formulations. Further, in relation to questions about the feasibility of deterring aggression in cyberspace, the advisory demonstrated that China was targeting critical infrastructure entities across all the Five Eyes nations, particularly communications infrastructure between the US and Asia, implying that the Chinese might be able to disrupt the ability of allies to effectively engage in any extended crisis, up to and including a cyberwarfare incident.

In sum, the advisory in May 2023 from the ASD (2023a) went into explicit detail not only in attributing the operation to Chinese APTs but also in exposing how the attack was conducted, and it provided public evidence of confidence in attrition capabilities in asserting with ‘high confidence’ who the attacker Volt Typhoon was as well as the state actor with which they were associated, namely, China.

4.8.2 LockBit 3.0

LockBit is a type of ransomware. A June 2023 advisory from the ACSC was about this particular ransomware-as-a-service update, with 3.0 as the newest version of a particularly virulent strain that has been involved in numerous situations across the globe including Australia (Australian Signals Directorate, 2023b). The ASD (2023b) advisory merits attention as it is publicly revealing its attribution capabilities to specific ransomware strains and also openly identifying certain indicators of behaviour around these.

Although it did specifically name potential aggressor nations, the advisory specifically mentioned that the malware was deliberately constructed to not trigger on 'systems with installed language pack for Commonwealth of Independent States (CIS) countries' (ASD, 2023b, p. 1). Listing Azerbaijan, Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan and Ukraine, the implication that LockBit was crafted in one of the Commonwealth of Independent States countries and the creator/s were either instructed or were aware that repercussions for affecting these nations are not worth the potential payload.

4.8.3 BianLian Ransomware Group

Another particular ACSC advisory in 2023 was part of a concerted effort to generate awareness in the Australian community about ransomware campaigns against Australian entities, but also doubled as a joint attribution advisory against specific Chinese actors (ASD, 2023c).

This advisory explicitly stated that the BianLian group is a cyber-criminal gang, and not necessarily related to China or CCP. However, BianLian had targeted critical infrastructure in Australia (ASD, 2023c). Unlike China's Volt Typhoon campaign, the BianLian ransomware group deployed tools in the targeted networked system that then conducted reconnaissance before deploying ransomware to shut the system down (ASD, 2023c).

Therefore, the ACSC signalled it was indeed aware of varying levels of sophistication in techniques among cyber attackers and that the ACSC and other Five Eyes agencies possessed the capabilities to accurately attribute and publicly disclose these identifiable cyber 'tricks' (Toulas, 2022). However, it is unclear whether this particular case resulted in the CCP acquiring any stolen data directly. Nonetheless, all these advisories covered a diverse selection of attribution reports in which the ASD and ACSC were directly involved, and all were significant in terms of deterrence and capabilities, in revealing a willingness to confidently 'name and shame' a cyber activity, including those originating from or with close ties to host states such as China. Although Australia has depended on the 'sophistication' of a cyber anomaly, the country appears to have the capability to attribute malicious cyber activity and align it with strategic responses, including political and diplomatic actions. With this in mind, and in light of the realities of attribution and Australian capabilities described, analysis in the next section will incorporate how this affects Libicki's framework.

4.9 Ramifications for Libicki's Deterrence Framework

First, the early information challenge is reliable and credible attribution, preferably within a short timeframe in which decision-makers can consider deterrence options and political actions, given the nature and extent of the effects of a particular sophisticated cyber attack.

Despite the forensic and related challenges of attribution, it has become apparent that open and public Australian responses to, and reporting of, cybersecurity incidents in recent years points to a growing ability to obtain accurate attribution with a degree of precision and speed. These attribution efforts have often culminated in the ACSC advisories and working within multilateral relationships such as Five Eyes, specific states such as China and even particular individuals have been labelled as responsible for malicious activities in various cyber incidents.

4.9.1 Do We Know Who Did It?

Ultimately, yes. As Cave et al. (2020) stated in discussing cyber incidents, there is

> an army of analysts in both private industry and government who work to understand the nuts and bolts of a breach or compromise. Over time, analysts collect clues about the people behind the compromises and that mass of information can lead to high-confidence attribution. Government intelligence agencies can use secret methods to achieve perfect attribution, but commercial entities can also achieve very high confidence.

As already mentioned, in Australia the ASD and the ACSC have taken the lead role in publicising attribution and advising and supporting response options to deter any such unacceptable behaviour in cyberspace. While specific operational details or precise timeframes of attribution are not openly determined in statements and advisories, question 1 of Libicki's framework is satisfied: Australia can determine 'who did it'.

Certainly, 'Do we *accurately* know who did it?' always will continue to have an interrelated question attached to it, which is 'Can we find out quickly?' to allow appropriate countermeasures. For deterrence by punishment, discovering the attacker with accuracy in a reasonable window of time to allow a credible and proportionate response is essential to giving decision-makers room for policy leverage and deterrence scope. Given the stated degree of seriousness about the nature of a particular cyber incident, a slow, protracted forensic investigation (even if eventually precise) has the drawback that any active deterrence response can be misdirected or misinterpreted by the original attacker (Libicki, 2009, p 97).

For reference, it is also worth adding that Australia and China have had a history of numerous cyber incidents that are not comparable to traditional kinetic operations but were still considered ‘serious’ enough for a strong, deliberate government response in the context of national security threats, and nations, including Australia, have repeatedly and openly rebuked the CCP diplomatically (Mann, 2023; M Payne et al., 2021). Again, this is as much a strategic and political consideration as it is a technical, forensic one. Consequently, it can be argued that deterrence for Australian policymakers in dealing with China will continue to be an art as well as a science.

4.9.2 Will Third Parties Join the Fight?

Australia cannot always act in isolation. For example, the Asia Pacific Computer Emergency Response Team is a grouping of national CERTs and Computer Security Incident Response Teams dedicated to the protection of national infrastructure in the Asia-Pacific region.

As highlighted in Australia’s International Cyber Engagement Strategy in 2017 (Department of Foreign Affairs and Trade, 2017b), this grouping is ‘just one example of economies collaborating to build collective incident response capability in order to prevent, detect, analyse, respond, mitigate and recover from cyber incidents’ (p. 26). The aforementioned cyber dialogue with India, and the equivalent with the US, also demonstrate that Australia is not exactly encouraging third parties to always join the fight but is at least collecting a network of potential allies who may step in under the right conditions, that is, conditions that attribution will play a crucial role in spurring (Department of Foreign Affairs and Trade, 2022; Nevill, Hawkins, & Feakin, 2017; Rudd & Smith, 2011).

However, in the development and application of international standards, a central impact of the ASD and ACSC advisories is the fact that they are often published in conjunction with Australia’s Five Eyes allies. Hence, it appears that Australia will continue to work closely with international partners to set standards and support technical capacity, albeit there is no formal obligation to ‘join the fight’ in kinetic terms. Perhaps the closest formal alliance commitment is that of ANZUS, which, since 2011, has been adopted to cover cyberspace and to support efforts to build better cyber resilience. As former Prime Minister Kevin Rudd asserted in 2011, Australia and the US ‘are committed to working together and with others to develop international norms to promote a safe, reliant and trusted cyberspace’ (Rudd & Smith, 2011).

Nevertheless, ANZUS is non-binding and does not guarantee that the US or New Zealand will automatically join the fight.

To this end, Australia should still treat attribution as its own responsibility and an activity that it must be capable of carrying out independently. Some ACSC advisories post 2022 have indicated that third parties will at least 'join in the attribution fight', but it remains uncertain whether they will join in a punitive response. Hence, Australia must also continue to develop and communicate the development of cyberwarfare capabilities to strengthen its deterrence-by-punishment positions further.

4.9.3 Does Retaliation Send the Right Message to Our Own Side?

Libicki (2009) pointed out that in the situation of retaliation, some cyber targets are government systems, whereas others are private—in fact in countries such as the US, most critical infrastructure is in private hands (p. xvii). This distinction is especially important for states such as Australia where the private sector is an intrinsic component of cyberspace. The ease with which retaliation can be executed against targets within another nation is a critical distinction for the cyber domain against the physical domain, yet it is rarely as catastrophic and, therefore, is unlikely to send a message of warmongering to a nation's own side.

Hence, the specific targets chosen for retaliation are important as they can shape the rules of engagement and potentially escalate the conflict, which Australia should take into serious consideration, given that a combination of factors will likely warrant retaliation to a cyber attack. As Gil Baram stated (quoted in Edwards & Handler, 2021), there is no secret formula

> for such a combination, as these circumstances will always vary from one case to the next, depending on many factors, such as the regime type and particular circumstances. It also depends whether this is a state-on-state conflict or one that involves non-state actors, since there are often different considerations for retaliation in each. Another thing to consider is visibility of the original incident. Whether or not the domestic or international public is aware of the incident may considerably impact the decision whether to retaliate and how'. (in Edwards and Handler, 2021).

Baram's argument is reflected in the ACSC advisories; for example, the advisory for the BianLian ransomware group differed from that for China's Living Off the Land campaign. BianLian was a criminal enterprise, and therefore, the mitigation recommendations in the advisory are perhaps about the extent to which deterrence will be carried out. That is, any

punishments would be attempts to pass on this information to Chinese authorities to then help in arresting the individuals. China's Living Off the Land campaign at this time had a similar response, but as the advisory stipulated that it is a state actor, the Five Eyes states can reserve the capability to respond in similar fashion.

Retaliation can also signal a message to the private sector in Australia itself. Deterrence strategies act as an umbrella response intended to protect the entirety of society, including the public sector. Removing the responsibility to react from the private sector is an important step as states should be responsible for the defence of the nation. Yet, Libicki (2009) argued that doing so can have a corrosive effect on private actors taking responsibility for their own cyber defences (p. 65). Therefore, as discussed in Chapter 2, an important step the Australian Government has taken is the creation of the ACSC and its reporting services for the private sector. The risk of publicly admitting an embarrassing cybersecurity event is ameliorated, there is greater coordination between public and private entities in Australia's cyber defences and private entities are given assistance to strengthen their cyber defences according to federal frameworks such as the Essential Eight.

This is ultimately a consideration for the decision-maker within the current political context, and simply put, once attribution is completed, then the Australian Government must exercise care in its response. The only clear limitations are that any attempts at retributive actions in the cyber domain should be limited to precise strikes that cannot, or at least the best efforts should be made to ensure these strikes do not, have cascading effects that Australian cyber operators cannot control—so that Australia can avoid escalation

4.9.4 Can We Avoid Escalation?

Avoiding escalation is a key consideration in cyber deterrence as there are many methods through which escalation can occur, not only through cyber means but also through conventional and even nuclear warfare methods (Libicki, 2009, p. 69). For Australian considerations, it would surely be considered an absolute failure of cyber deterrence were escalation to cause strategic conflict to leave the cyber domain.

Escalation can occur for many reasons. It can occur if the attacker believes the cyber anomaly was the result of a deliberate malicious action (rather than innocent human error) or that a cyber retaliation was not merited or disproportionate, and if they face internal pressures to respond in a certain aggressive way or believe they would lose in a cyber tit-for-tat exchange but believe

they could win in other physical domains where they enjoy superiority (Libicki, 2009, p. 69). For states such as China, where saving face is often considered imperative to the CCP's survival, the internal pressures can become particularly problematic in the event of a cascading effect of cyber attacks that might spill over into the public domain and become common public knowledge (Zhou, 2020).

Nevertheless, avoiding escalation will also allow a deterrence-by-punishment framework to be effective. That is, if the adversary is deterred immediately and is not so recalcitrant as to fire another salvo in response, then the deterrent mechanism has succeeded as the default option. The manner in which Australia would avoid escalation when responding with deterrence by punishment against China is also complicated by frayed diplomatic relations, including a lack of trust, between the two states, which is balanced by close economic ties that have immensely benefited both (Clarke, Hsu, & Peng, 2023). In summary, the strategic calculus of Australia will continue to weigh potential Chinese economic and diplomatic retaliation with potential deterrence and associated benefits.

In this sense, Australia's aim is not only to have accurate attribution but also to attempt to ascertain the motive behind the cyber anomaly in the backdrop of geopolitical developments. Australia also does not need to have a dominant cyber force that can completely overwhelm the Chinese cyber apparatus. It needs the perception-based power to simply deter malicious cyber activity by the Chinese state via cost–benefit analyses (Scott, 2022). As explained in Chapter 1, deterrence is an effort to shape the strategic decision-making of a potential adversary. Deterrent mechanisms are often viewed via the perspective of the state that is deterring, but the value of those steps will also depend on their effect on the perceptions of the target state. Then, Australia will also need to shape the perceptions of China so that the state sees the alternatives to aggression and coercion in cyberspace as more attractive.

In essence, Australia should emphasise and communicate imposing costs on malicious actions and keep perceptions around those costs credible and in sufficient proportion such that it does not immediately escalate the situation further. Rather than focusing on crushing opposition in a potentially harmful conflict, shaping perceptions so that an adversary such as China can see the alternatives to cyber aggression is an optimal and achievable strategic outcome.

In addition, Australia has been consistent about 'rules of the road' and stability in cyberspace, with former Home Affairs Minister Karen Andrews (2021) publicly adding 'all countries –

including China – should act responsibly in cyberspace'. In the same statement, Andrews (2021) also posited that Australia would report cyber incidents and attribute them, 'especially those with the potential to undermine global economic growth, national security, and international stability' (Andrews, 2021). The implication is that Australia's objective is not cyberspace dominance, but instead, embarking on actions that cause expectations that other states will adhere to 'red lines' and codes of conduct that benefit all states in the cyber domain.

4.10 Summary

This chapter illustrates a clear point—attribution is possible and 'Do we know who did it?' is an answerable question with 'satisfactory' levels of evidence to support it. It is difficult but attainable forensically, tactically and strategically. It also acknowledges that attribution remains a political problem as well as a technical one.

There is an evident attribution policy progression in Australia. It was once an actor hesitant to 'name and shame' malicious entities; now, it appears to have changed its political mindset and policy approach and has become far more confident to attribute malicious cyber actions to China. It is also clear that Australia is willing to act collectively with the public support of allies, perhaps in the hope of avoiding escalatory counter-retaliation. Therefore, the answer to the question 'Do we know who did it' appears to be affirmative in broad policy terms, and 'Does retaliation send the right message to our own side' has a baseline and precedent from which to work.

Certain difficulties are encountered in attribution because it is reliant on these interrelated methods to become truly reliable and to be seen as credible. Forensic methods can be, and routinely are, frustrated. Tactical methods without forensics are hearsay and may be speculative projection, even if strongly informed by reasonable assumptions. The strategic analysis of attribution becomes postulation without being informed and guided by these two methods.

Thus, the Australian Government's position on attribution has habitually been open-ended, as described by former Minister for Home Affairs Karen Andrews in 2021: 'Australia publicly attributes cyber-incidents *when it is in our interests to do so* [emphasis added], especially those with the potential to undermine global economic growth, national security, and international stability'.

Yet, it is because of this fluid conflagration of methodologies that attribution is neatly summed up sometimes as art and sometimes as a science. However, the findings of this chapter show that attribution should be viewed as science being conflated with art—the marriage of forensic investigation with strategic and tactical analysis, which enables varying levels of attribution. Significantly, if every cyber incident is labelled as 'sophisticated', then nothing is, and the lens of sophistication can be misleading.

Public developments of attribution are themselves statements of intent and have enabled Australia to contribute to allied responses and ensure that it is not simply a beneficiary of its allies' capabilities. This aspect is especially important to the investigative framework, as Libicki asked whether third parties will join the fight as well as the message it may send to our allies. The current position of involving the Five Eyes alliance from the outset is good practice in that it strengthens attribution at all levels discussed just prior and means that the Australian Government can speak with confidence publicly about nefarious Chinese activities in the cyber domain, such as in July 2021, when Australia formally attributed the Microsoft Exchange software cyber attack to China.

In summary, Australia has established attribution capabilities that can identify threats and give decision-makers a strong degree of confidence in whichever policy pathway they embark upon, including to impose costs on state-based (or state-sponsored) actors such as China. Although Australia does appear to possess rapid and robust attribution capabilities, such technical advancements will always be combined with political assessments to 'name and shame' and political calculus about the 'sophistication' of any cyber incidents.

Attribution is thus 'what states make of it', but Australia's commitment to investment and capacity building in areas such as public–private partnerships, its revised standards of practice in the cyber domain, including to publicly disclose attribution, and the building of international alliances or agreements in a coordinated fashion all indicate that policymakers, the ASD and the ACSC can confidently and reliably conduct attribution and a 'whodunit' investigation. The capability of these entities will be essential for then breaking down Libicki's (2009) framework in the next chapter to explicitly investigate Australia's capacity to deter malicious Chinese activity in the cyber domain specifically through deterrence by punishment.

Chapter 5: Deploy Payload—Destroy, Disrupt and Degrade Target Enemy Networks

Cyber deterrence is not a static solution. This chapter breaks down Libicki's (2009) deterrence-by-punishment framework proposed in C*yberdeterrence and Cyberwar*, with a focus on deterrence postures and the relationship between Australia and China. The intent of this case study is to deploy the research and analysis of previous chapters and the context that has been established and then to deploy analysis in functional terms, in order to argue the applicability of deterrence by punishment in the cyber domain and whether this framework for inflicting 'unacceptable' punishment is of utility to Australia.

This case study analysis is also informed by public policy analysis, and understands that "…solutions for practical problems demand much more than the analysis of rational choice, expected utility, and opportunity costs" (Dunn, 2015, p. xvii). In short, the analysis also considers that deterrence is the imposition of psychological effects on a potential adversary to affect their strategic decision making. Policies are the set of forces within the control of the actors in the policy domain that affect the structure and performance of the system (Walker W, 2000 p. 13).

From this, the strengths and weaknesses of offensive or retaliatory strikes against China can be determined, including the challenges of showcasing cyber capabilities as a deterrent, the dangers of unintended escalation, restrictions on actors such as Australia regarding the available scope of punitive activities through target analysis and the way that all these factors will influence Libicki's deterrence-by-punishment framework.

As Libicki (2009) stated in *Cyberdeterrence and Cyberwar*, deterrence by denial is preferable, but deterrence by punishment should not be ignored, underplayed or overlooked (p. 7). This is because, in part, deterrence via denial alone is difficult to sustain over the long term. As stated, deterrence by denial is the ability to frustrate cyber actions and is informed by the principle that 'if cyber-attacks can be conducted with impunity, the attacker has little reason to stop' (Libicki, 2009, p. xvi). Alternatively, deterrence by punishment signals to a potential attacker that there will be significant and substantial punishment in retaliation for an attack. In reality, there is no true restriction that retaliation should remain in the cyber domain; however, for Australia, limiting strategic contest against China to the cyber domain is favourable.

Of note, deterrence by punishment also entails a persuasive psychological element. Hence, the key focus of the chapter will be on how, and to what extent, Australia can deter major cyber attacks on itself via a deterrence-by-punishment policy. In particular, it will revolve around the themes of communication (signalling) and capacity in adapting deterrence efforts to the most efficient level in a changing cyber environment. It will also contribute to finding proportionate real-world responses, both from what is publicly available and theoretically possible.

Further, attribution has been discussed and unpacked in Chapter 4, which, in part, has illustrated the difficulties in differentiating between potential targets for retribution. In short, retaliating against the wrong actor will be highly counterproductive. Nonetheless, a critical consideration for Australia regarding deterrence-by-punishment mechanisms involves deciding how decisive and proportionate the response will be. This type of question does lead into the core questions posed by Libicki (2009) himself. Does this response send the 'right' message to our allies? Will it avoid unintentional or unreasonable escalation? In the Australia–China context, Australia is comprehensively outgunned in the kinetic domain, and thus, restricting escalation and keeping strategic competition in the cyber domain is a critical component of any deterrence-by-punishment strategy. Therefore, defining just what the Australian Government could target in a deterrence-by-punishment context is useful for categorising the effectiveness of deterrent mechanisms.

Simultaneously, it is self-destructive to explicitly state what a cyber weapon can do before it is deployed, as the potential aggressor (here, China) that Australia is attempting to deter might pre-emptively investigate and harden their systems and patch or fix whatever vulnerabilities Australia has announced they could hit as punishment. In this sense, specific cyber targets need not be disclosed. Therefore, deterrers such as Australia lack the ability to always signal intentions unambiguously and/or openly declare the precise Chinese assets they may hold at threat in retribution. Yet, without clear communication, deterrence by punishment may also be viewed as lacking credibility or can be so vague that it can lose (psychological and political) potency. In the other areas of deterrence, such as nuclear deterrence, the demonstration of nuclear weapons has often functioned as the communication of technical capability (Sanchez E in the UN General Assembly, 2023). The investigation of potentially similar demonstrations in the cyber domain is crucial, such as Exercise Cyber Sentinels, which will be unpacked later in the chapter (ADF, 2023). Therefore, the central findings of this chapter address this paradox

and will be heavily influenced by the communication difficulties of deterrence in the cyber domain, which are driven by a lack of specificity.

5.1 Australia, China and the Logic of Retaliation

In the context of this thesis, threat rhetoric and the blunt shaping of a physical battlefield to encourage a direct confrontation with China are highly improbable policy actions and strategic objectives. The relationship between China and Australia can be fractious but is also multidimensional and complex with large economic, political and social cooperative facets to it. In short, the two countries are dependent on each other. For instance, in the economic sphere, Australia supplies '61 per cent of China's iron ore, 53 per cent of its coal and 23 per cent of its thermal coal. Australia's shares in each are increasing' (Triggs, 2019). This may only represent a small section of the economic entanglement between the two states, but the sheer scale of iron ore, coal and thermal coal alone underscore how the relationship is tied by crucial commodities. Therefore, both states engage in efforts to established normative and peaceful response frameworks. While competition is evident, including persistent Chinese cyber-espionage campaigns that fall short of thresholds of violence, the outbreak of kinetic war is equally undesirable to both actors.

Given the application of conventional thresholds to cyberspace, and if China does cross a 'cyber red line', this scenario could certainly lead to an over-reliance or acceleration of aggressive rhetoric. Nevertheless, as Foreign Minister Wong stated in 2023, there is a strategic competition in the Indo-Pacific region on several levels—economic, diplomatic, strategic and military—all are interwoven, and all are framed by an intense contest of narratives. Yet, Wong (2023) also emphasised peace through diplomacy, the importance of international law and that ' those interests lay in a region operating by rules, standards and norms, where a larger country did not determine the fate of a smaller country, and where each country could pursue its own aspirations and its own prosperity' (2023).

Further, according to Wong (2023), the conditions for stability and peace through diplomacy in the Indo-Pacific would incorporate 'playing our part' in the collective deterrence of aggression. Therefore, being able to deliver deterrent effects would call for nations to enter into partnerships in order to preserve order and ensure peace and prosperity. Some like Rory Medcalf have even argued that in future, a collective Indo-Pacific block may have the power to challenge the influence of China—the proliferation of new agreements such as AUKUS, the

Quad, the strategic cyber dialogues between Australia and states such as the US and India (both described in Chapter 2) constitute interdependent parts and show how states are coalescing to potentially challenge and change Chinese influence (as cited in Galloway, 2021).

Even if or when Australia and its allies are able to hold China's forces and infrastructure at risk, the main goal is deterrence in order to decrease the risk of conflict rather than to provoke China into a deliberate and direct kinetic confrontation. In broad terms, the 2023 Defence Strategic Review marked an important shift in Australia's approach to China and placed a significant emphasis on the adoption of deterrence strategies to deter aggression (p. 37). Therefore, deterrence by punishment in the cyber domain will occur with the deliberate intent of engaging in cooperative defence activities and shaping potential adversaries' behaviour based on agreed rules and, in part, by cyber means. Defence contributes to integrated deterrence and will then allow room for the de-escalation of tensions and the search for common ground while potentially imposing a severe cost on any major power that might consider attacking Australia. It will also require adapting to current and changing strategic circumstances and assessments. Indeed, in Australia's case, some have argued that past decisions not to call China unequivocally responsible for particular cyber attacks seems 'to have been out of concern that exposing the cyber attacks would require escalation in other parts of the relationship with China, most notably in the domains of trade and finance' (Farley, 2019). However, with the above considerations about economic entanglement affecting not only Australia but also China, this may not explicitly be the case. Australian deterrence considerations are about making aggressive actions against Australia prohibitively expensive (Department of Defence, 2023, pp. 6, 37). With the scale of economic entanglement between Australia and China, the concerns about their strategic-level cyber competition escalating into the cyber domain, although very legitimate and worth considering always, may not actually be as dire as at first considered.

5.2 Deterrence by Punishment and Decision-making in the Cyber Context

Overall, the significance of deterrence by punishment is that the threat of a retaliatory strike, or perhaps the shaping of a potential future battlefield will influence the future operational and strategic considerations of a targeted state. Moreover, any deterrence response should aim to be timely and proportionate. The closer the time of retaliation to that of the initial 'unacceptable' cyber attack, the more likely the attacker will correlate the two and understand that by conducting selected operations there will be certain punitive or related responses, the concept of temporal continuity and contingency, the notion that the further away a punishment

is from a deed the less impact it has on decision-making (Staddon & Cerutti, 2003). This is important, as the retaliation in itself does not necessarily have a diplomatic or explicit communicative aspect; however, the retaliation should not be so delayed that it might appear to be indiscriminate or conducted at random—and perhaps then provoke states in becoming embroiled in a muddled tit-for-tat exchange (Libicki, 2009, p. xvi).

Similarly, in the cyber domain, even if the attacker is caught, often the expected gains of an attack will completely outweigh the associated or cumulative pains of the attack owing to a lack of norms enforcing consequences (Lewis, 2022). It is rarely that expensive to conduct offensive, malicious cyber operations, unless it is something incredibly bespoke and unique such as Stuxnet, which according to former CIA Director, General Hayden, cost about US$1 million (Flanagan, 2011). If a public punishment mechanism is lacking, and the cost of even the most publicly acknowledged and advanced cyber operations is sufficiently low, the threat of retaliation is necessary and should persuade the attacker that the possible rewards are negligent and that there is sufficient evidence to inflict retribution if they are caught. For these reasons, the attribution challenge is considered so important in not only this thesis but cyberwarfare in general. Rapid attribution is a crucial aspect of deterrence by punishment owing to temporal continuity and contingency (Staddon & Cerutti, 2003). Indeed, along with the need to avoid misplaced punishment, even when

> one has properly identified the culprit, it may still be a strategically sound choice not to pursue attribution and punishment … the consensus of onlookers is an important feature of deterrence. A high level of public attribution is necessary to convince the culprit and the international community that the retaliation is justified and acceptable within the bounds of the UN Charter. (Nevill & Hawkins, 2016, p. 12)

In considering deterrence by punishment as a policy response contributing to an overall strategy for Australia to deter China from launching cyber attacks, it is necessary to note that Libicki (2009) raised the risk of escalation, as did others (e.g. Ranger, 2019). This risk could directly correlate with real or perceived temporal advantages and an increase in aggressive rhetoric that might encourage pre-emptive cyber offences (Ranger, 2019). This risk of such international misunderstandings is problematic as deterrence communications should primarily be about preventing or mitigating the outbreak of conflict and therefore not undermine the diplomatic platform to intimidate in the future. Again, in short, the presumption is that neither Australia nor China wants to start a conventional war with one another, yet any missteps can be

escalatory. In this sense, Australia can and should act unilaterally to mitigate the risks, which will involve calculations of policy restraint.

Another overlapping component of deterrence by punishment, which is associated with governing cyber capabilities, is the provision of a proportionate technical-finding tool that decision-makers can employ without immediately creating an escalation crisis, for instance, by investing in the capabilities needed to ensure that cyber espionage is not mistaken for a cyber attack (Perloth & Sanger, 2019). Decision-makers should also definitely consider the unique characteristics and effects of cyberwarfare that could entail the risks of unanticipated collateral effects as well. Hence, the likelihood of collateral damage might be quantified and the need for proportionality could still assist with damage limitation. As Acton (2020) clarified:

> Part of the solution should be to ensure that the assessment of escalation risks is not narrowly confined to the military or intelligence personnel responsible for proposing, planning, and conducting cyber operations. Such personnel are generally not trained in estimating – if an adversary detected a cyber operation – how threatening it might perceive the operation to be and how it might react. Rather, a broader cast of experts, including intelligence analysts who specialize in understanding foreign decision-makers, should be involved. In this context, this essay and other academic works hopefully have a role to play by identifying and raising awareness of the potential risks. (p. 144)

Retaliation needs to threaten enough harm to prevent an attack but not trigger an escalation crisis, which often implicates proportionality and a cost–benefit framework (Nevill & Hawkins, 2016, p. 6). Such retaliation might also rarely involve a perfectly identical proportionate response to the incident itself, but the threat of retaliation must be credible enough to affect the psychology of the actors involved. Thus, retaliation can encourage behavioural norms.

5.3 Different Threat Actors

Overall, deterrence by punishment in the cyber context could be considered as deploying mechanisms at the strategic, operational or tactical level. Thus, when considering deterrence by punishment a key question arises: Who must be punished? For Australia, the variety of groups that can be considered targets for punitive measures can be individuals, networks, groups and China’s state apparatus itself. Nonetheless, all these targets must have something of value for a retaliatory strike to be effective.

These four categories have been selected as they are distinct and discrete, despite often having some overlap with one another. They have varied punishment responses that can range from more normative legal or diplomatic penalty mechanisms such as arrest warrants to the threat of large-scale infrastructure damage that might be capable of directly influencing the perceptions of high-level decision-makers in China (ASD, 2023). Such threats will be consigned to cyber activities only for clarity and are inherently constrained by geography. Critically, as stated, different punishment strategies might have to be applied to different actor targets. Further, in broad terms, the target must understand that the retaliatory act is a direct result of the offending deed.

Individuals could be useful as targets for retribution for various reasons. Not only may the individual be rendered incapable of perpetrating further cyber attacks, but they could also function as a message to other like-minded individuals. Concurrently, targeting the individuals may send a legal message to a host state, as illustrated in 2014 when the US issued five arrest warrants for persons in the PLA over a cyber-espionage incident in order to hold China itself accountable for the cyber attacks that their proxies had conducted (Schmidt & Sanger, 2014). The advantage of targeting individuals in a criminal sense is that attribution can take longer in order to avoid ambiguity while still functioning as a deterrent mechanism that signals a resolve to punish aggression (while the legal threat must be credible). Such credibility is advanced by establishing the reasons for arrest, which are explicitly stated when warrants are issued. Thus, the individuals will know the precise transgression for which they are being targeted and that their clandestine operations can and will be attributed.

This is especially relevant in cyber deterrence as the speed of attribution and retribution is a noted issue. If retribution takes too long or is too ambiguous, the actor facing retribution may not collate the action with their prior transgression. Given that cyber capabilities are not always easy to showcase, Libicki (2009) argued that, especially for state-to-state dealings, ‘deterrence delayed is nearly tantamount to deterrence denied’ (p. 98). Thus, legal signalling has its limitations in terms of scale and effects in that it can suffer from time lags, limit operational flexibility and not necessarily have an immediate impact on the target’s operational considerations. Thus, criminal prosecution and posturing that aims to reinforce international law is likely the most significant option in which long-term attribution will be most effective to inflict a normative-induced punishment and legal framework.

Significantly, Australia's involvement in 2021 in unsealing arrest warrants alongside US counterparts—in a separate matter to that noted above—for Chinese individuals showed its willingness to engage openly to prevent escalation and certainly demonstrated to China that Australia did have the capability, allies and abilities for successful attribution (M Payne et al., 2021). Deterrence by law enforcement has another advantage, in that 'in addition to tackling threats from external parties, it curbs malicious insider threats which are often difficult to anticipate and pre-empt, and which are on the rise globally' (Hui et al., 2017, p. 36).

In terms of groups, this would involve the targeting of APT, teams of intruders and continuous and sophisticated hacking techniques with significant resources, which is a step up from targeting the actual individuals located within them. Australia must take retributive actions against groups that conduct malicious operations, or these groups may become emboldened to continue harassing Australian entities and interests, which Australia already does through entities such as the ASD and AFP (ASD, 2023; Department of Home Affairs, 2023, p. 8). Such groups are not confined to APTs of course, and the phenomenon of 'patriot hackers' also presents a significant problem to deterrence strategy. Patriot hackers provide a distinct advantage in that they are an unofficial crowd-sourced grouping, and it is unclear how they receive support or direction. They operate in 'a legal gray zone, as they are neither explicitly civilians nor combatants. This ambiguity is useful for authoritarian governments since they can shift responsibility for cyber-attacks on Western targets to patriotic hackers' (Young, 2022). Consequently, a significant advantage for states such as China is that they can eschew responsibility for cyber attacks and instead insist that these rogue elements within their borders are conducting hacking or related operations and that the state is not culpable. Indeed, it has been argued that Chinese state security services and military entities have increasingly contracted hackers to carry out cyber-criminal activities abroad (Young, 2022). In short, Chinese patriot hackers are being blamed for an ever-increasing number of cyber attacks while the CCP is suspected of employing an army of hackers.

Moreover, patriot hackers form indistinct and constantly fluctuating organisations, but their actual impact is contestable. Any advantages of covert operations committed by patriotic hackers often only derive from these being primarily aimed at rallying and spreading nationalist expression. Hence, it can also be argued that with the dominant control China has over its sovereign cyberspace, its claims that patriot hackers are operating outside of CCP control has limited value (Sigholm & Bang, 2013). Moreover, China is not exempt from 'effective control'

or *lex generalis*, the principle imputing state responsibility for the unlawful actions of non-state actors (Stockburger, 2017, p. 1).

Given the widespread use of items such as DDoS attacks and distributed malware attacks to promote nationalism rather than to achieve strategic objectives, networks are an interesting target for retaliation. The reason networks are described as 'interesting' is that the targeting of critical infrastructure is often seen as a significant red line for states, as illustrated in the infamous 'missile down one of your smokestacks' threat—an initial US strategy that was intended in part as a warning to adversaries that may attempt to sabotage electricity grids or pipelines (Gorman & Barnes, 2011). The targeting of power stations and grids is a common trope in the discussion of cyber attacks and retribution, and perhaps represents the most likely attack scenario involving strategic cyberwarfare operations and new types of conflict. Despite this and given that the barriers to entering cyberspace are extraordinarily low, such retaliatory framing on shadowy patriotic networks again raises many questions about proportionality. That is,

> An attack on a military system is one thing—and it might presage a physical attack as well—but if a civilian target such as a power grid or bank is taken down, does that justify a military response such as a bomb on a physical facility, with likely lethal consequences? (J H Davis & Sanger, 2016)

Australia's allies have also cast aspersions on how it should react to critical infrastructure being crippled by a cyber attack, as demonstrated in 2021 with the ransomware attack on the Colonial Pipeline that forced the company to shut down a 5,500-mile-long oil pipeline (Perloth & Sanger, 2021). This attack has been attributed to DarkSide, a Russian ransomware group that is 'plausibly tolerated by the Russian government' (Rivero, 2021). The incident is instructive to Australia of a criminal enterprise operating in a foreign nation causing strategic-level effects on energy and resource supply chains via a cyber attack, and the response from the US was not to trigger a public cyberwar. Therefore, in considering how retaliation would appear to their side, Australian decision-makers should consider such events, or Australia and her allies would need to ensure clarity about their responses to such events from 2021 onwards.

Davies (2016) added that such cyber attacks are not always obvious and that 'Even if the location from which an attack is launched can be reliably discerned, there's still the issue of who was responsible; was it state-backed, a "citizen's militia" or just an individual?'. Given this confusion in thinking about cyberwarfare, patriot networks can be seen as a troubling target

choice owing to issues such as the possibility of mistaken identity and reasons that might lead to unwanted, disproportionate damage. In addition, power grids can fail or be disrupted (e.g. by natural disasters or human error) for all sorts of reasons and not just because of a deliberate cyber attack by a foreign entity. Any lowering of the bar for a collective defence response to cyber attacks would need to access the both the motivation and sophistication of the attack and, therefore, address the merits of expanding the triggers for punishment or cross-border policy responses.

> If aggression in cyberspace is not tied to actual physical harm or threat to lives, it is unclear then how we should understand it. Does it count as aggression when malicious software has been installed on a computer system that an adversary believes will be triggered? (Lin, 2012)

Libicki (2009) also discussed the option of retaliation *sub rosa*, or in secrecy, as a viable option for state-on-state cyberwarfare operations (pp. 94, 128). *Sub rosa* cyberwarfare can potentially limit escalation (which is affected by the particular cyberwarfare operations undertaken, of course), perhaps keeping the conflict within the cyber domain although it is unclear how discriminatory cyberwarfare might be. Therefore, conducting said operations with full public statements supporting punitive responses (and condoning the initial network attack) must be addressed across the entire crisis-management spectrum. Therefore, punishment planning is related to the understanding of how the CCP itself would perceive the escalatory aspect of potential offensive operations on groups such as patriot hackers, even if conducted in secrecy.

In efforts to understand the parameters of any cyber attack, networks can be designated as critical infrastructure because of the infrastructure's ties to classified defence or sensitive government networks. This applies to any digitised society and not just Australia and China. Networks can also be tied to the functioning of strategic assets such as electric grids and power sources; Australia has an ever-expanding list of such assets (Department of Human Affairs, 2023). Therefore, an attack on networks that intends to destroy or debilitate their functions bears the risk of being assessed as an attack on the state's ability to function effectively and defend itself. This is a conundrum but a worthwhile consideration. Libicki's (2009) own comment on it is that critical state-based infrastructure functions present unique opportunities for attack and particular assets present distinctive, interconnected vulnerabilities that could be held at risk (p. 129). Such sectors have increasingly become more reliant on deterrence-by-denial logic and related solutions to prevent damage.

Overall, both policy adaptation and analysis regarding deterrence targets will remain very important. Networks, industries, people and the state are also all becoming increasingly interconnected, and potential tools or threats of punishment will affect the strategic considerations of state actors, which creates overlapping questions about the proportionality of response and different types of cybersecurity (Bajkowski, 2023)

As noted, an associated challenge is whether data collection and attribution alone can determine target identification and who might be punished as a 'just-right' response. As explained in Chapter 4, the attribution problem is brought up as an inhibitor to the deterrence strategy. Attributing an attack correctly and quickly in a specific context is part of an overall deterrence menu and will be extremely important to deterrence by punishment, including if the threatened punishment may be perceived as too disproportionately punitive to be even credible.

Nonetheless, this does not mean that deterrence calculations do not necessarily presume a high order of calculability. For example, the attacker is the one who will also draw from their own data and calculate the risks from aggression. This will come into consideration when dealing with phenomena such as patriot hackers and unaffiliated hacking groups. That is, is China (the aggressor state) willing to accept unaffiliated hacking groups, or patriot hackers, and the affect they may have on risk assessments by Australia and how Australia could respond to malicious activity? A host state such as Australia may also not have conducted the offensive cyber operation, but this should not necessarily then remove the doubts of China from future considerations of retribution particularly as the amount of damage that can be credibly threatened might transform over time.

Determining who will be struck by the retributive mechanism, maybe in the backdrop of the non-obviousness of the immediate threat, is important when considering the strategic value of state actors. Through deterrence, as discussed in Chapter 1, an attempt is made to influence the strategic decision-making of an adversary. What must be ensured is that the act of retribution is linked to a specific action and has obvious connectivity. Such options in the cyber domain will also depend on the scale of deterrence. That is, 'The existence of a deterrence scale associated with the response to a particular bad act, below which any particular reprisal threat may be too weak and above which any particular reprisal threat may be too costly or non-credible' (Libicki, 2018, p. 45). Last, the retributive action must be proportionate not only to control escalation but also to manage credibility itself—if the threat is too drastic from

Australia, then Chinese decision-makers may consider that it is impossible for Australia to achieve the threatened effects and that the threat should not be taken literally.

Ultimately, should Australia deliver retribution for alleged cyberwarfare operations by the CCP, Australia should consider whether attribution is timely and precise, and its policy options should not follow a 'one size fits all' model. Nye (2019) argued that deterrence in cyberspace is similar to preventing crime: 'governments can only imperfectly prevent it'. Nye also added that over time, 'better attribution forensics may enhance the role of punishment; and better defenses through encryption or machine learning may increase the role of denial and defense [sic]' (2019). The main lesson for policymakers is to focus on the most important attacks, ignore some of the attacks some of the time and if initiating any retaliatory strike, it should be informed by the original action from the aggressor. Otherwise, the response could be confusing and disproportionate and lead to unintended escalation.

5.4 Deterrence and Punishment

Deterrence in cyberspace can never be perfect or unqualified but is driven by cost–benefit calculations. The same logic applies both to potential attackers and defenders and addresses both broad-spectrum behaviour and specific acts (Morgan, 2003, p. 44).

As captured by Mazarr (2018), deterrence by punishment can threaten severe penalties while 'deterrence by punishment is not the direct defence of the contested commitment but rather threats of wider punishment that would raise the cost of an attack' (p. 2). Hence, in dealing with real-world situations, deterrence can incorporate cyber and non-cyber policy options, including legal, economic and diplomatic approaches as part of the threat of retaliation, and this is already the position taken by Australia via successive cyber strategies (Department of Home Affairs, 2020, p. 27; 2023, pp. 20–21). Thus, deterrent threats need not be restricted to cyber responses.

As discussed, the effectiveness of different deterrence mechanisms depends on context. Further, not all cyber attacks are of equal importance, which may have informed Australia's 2020 strategy and the assertion that attacks may not even be responded to if it may cause unnecessary escalation (p. 26). This gives the Australian Government strategic flexibility. Deterrence should have a psychological effect that plays on the mutual vulnerabilities and interdependent relationships between two or more actors, hence the term relational variable.

This psychological impact will depend on an opponent's assessment of credibility, capacity, proportionality and possible cost–benefit consequences. In other words, an actor such as China must receive (i.e. receive communication, which is discussed in the next section) and consider the threat of punishment as legitimate and conceivable. This view will be driven by various policy instruments of Australia's international power projection, which incorporate what CCP assets can be held at risk and for how long. Australia's positioning to give strategic flexibility is useful to it in supporting credibility when it does decide to make a threat.

Compounding this relational variable in intra-domain retaliation are the external political, social and economic realities of the domestic setting that the actors involved find themselves exposed to (Gray, 2000). Therefore, punishment threats must again be both timely and appropriate/proportionate as political calculations and domestic pressures will, and do, tend to play a large role in the cyber era. The elevation of cyber norms of good behaviour may also help to raise the reputational costs of bad behaviour. This is important as there is always the possibility that no matter how robust a deterrent mechanism may appear in theory, it may simply not work as intended on application. The construction of deterrence-by-punishment mechanisms are not only a technical matter but also a political, strategic and operational question. For instance, planning exercises alone 'would be valuable, forcing a whole of government consideration of the true costs of cyber-attacks and what steps we are truly willing to take to stop them' (Fitzgerald, 2015). Exercises such as Cyber Sentinels between the ADF and US military cyber experts are a strong public demonstration of both implied capability and of a third party that would likely join the fight (Department of Defence, 2023). Simultaneously, as actors develop a more sophisticated understanding of the costs and as threats become more easily identified technically, the political perceptions of the benefits of deterrence will become more embedded, at the very least in normative considerations.

Such open training and collective defence can be seen as, in part, an investment in military assets to provide Australia with an asymmetric capability against future adversaries. Such military manoeuvres are public and are often deliberately presented in diplomatic terms and subsequently deliberated upon by potential adversaries in conducting a cost–benefit analysis for a future attack. Therefore, it is worth reminding that the execution of cyber weapons is often silent, subtle and discrete unless they were deliberately and calculatedly deployed not to be so (Libicki, 2009, pp. 15–16). This silent dimension again points to the ongoing need to clearly communicate desired cyber-deterrence postures, by first acknowledging capability, which

might exist alongside joint military exercises with the US and other nations. This might also entail distinguishing between military and non-military roles.

At the least, a strong dimension of 'cyber learning' will remain imperative. As Nye (2019) stated, as state actors (and non-state ones)

> come to understand better the limitations and uncertainties of cyberattacks and the growing importance of the internet to their economic wellbeing, cost-benefit calculations of the utility of cyberwarfare may change. Not all cyberattacks are of equal importance; not all can be deterred; and not all rise to the level of significant threats to national security.

5.5 Communication, Capacity and Deterrence by Punishment

Actors must continually communicate on matters related to cyber conflicts and deterrence postures. While communication alone cannot address the growing cyberspace threats, effective and consistent communication within a cyber-deterrence framework can act to support and strengthen related capability and credibility components. Regardless of the specific costs Australia might seek to impose, it will need to develop and communicate stronger deterrent actions towards China. Significantly, the US and other like-minded actors have even issued statements in reaction to intelligence alerts about the detection of *impending* cyber attacks and then warned that such actions would result in consequences. Hence, a key is what exactly is being communicated: In other words, what is Australia verbalising and then executing?

For example, in 2019, US officials described the previously unreported deployment of US computer code inside Russia's energy power grid, with then National Security Advisor John R. Bolton publicly adding that there would be a 'price to pay' for engaging in cyber operations against the US, specifically naming Russia in the process (Perlroth & Sanger, 2019).

Ultimately, while Bolton declined to disclose specifics, the US statement insinuated that there was already a malicious code within Russian power grids, which could be deployed should Russia provoke the US into doing so, or that vulnerabilities in the systems had been discovered that US offensive teams knew how to exploit. This was most likely in response to Moscow's disinformation and hacking units around the 2018 US mid-term elections (Barnes & Sanger, 2021. Regardless, it was a clear statement that US strategy had shifted more towards an offence posture with the deployment and placement of potentially crippling malware inside the Russian grid system and other targets. This dimension of deterrence by punishment also points to

‘implants’—software code that can be used for surveillance or attack—inside targets that already had been deployed, but not activated (Barnes & Sanger, 2021).

Simultaneously, by being so blatant about the costs and risks faced by the perpetrators, Bolton could have arguably been providing geopolitical crisis ‘off-ramps’—a diplomatic pathway that both powers could engage in and potentially defuse a situation by having the consequences of an escalated offence–defence scenario to address. It also placed questions of cyber deterrence within the wider context of escalation and deterrence, potentially occurring simultaneously in multiple domains. Consequently, the threat of cyber weapons can be seen as useful in shaping the initial stages of a looming crisis in a manner that produces bargaining and risk assessment benefits; the inference from this process is that the presence of a proposed cyber response does not automatically cause escalation (Jensen & Valeriano, 2019).

Rather, the clear communication of desired actions and outcomes can allow openings to identify the risk or negative results more clearly for actors if they do not modify their cyber behaviour. According to Jensen and Valeriano (2019), ‘Modern crises bargaining involves a mix of overt and covert cross-domain signals states use to manage escalation and provide options that might help them advance their interests short of war’ (p. 2). Such cyber tools should be deployed alongside *sub rosa* communications to indicate that, for example, while Australia would desire diplomatic and peaceful solutions to a particular crisis, Australian decision-makers do have a layered cyber-deterrence strategy, have established thresholds and are also prepared to deploy the offensive cyber options available to them. Bolton’s threat of destabilising Russian power grids has also been seen as an example of cyber deterrence through capability and credibility (Filkins, 2019).

Ultimately, deterrence by punishment in the cyber domain practically rules out the traditional MAD principles, but it is not necessary to compare cyber deterrence with nuclear deterrence. Countries such as Australia can provide clear messages that they are willing and capable to act pre-emptively or provide some form of punishment if they detect an imminent threat of cyber attack. This might restrict the activity, rather than offering one significant event that deters a possible attacker, a sustained and recurring strategic loop that must be constantly engaged in to be effective. As stated, this will also demand a capable and credible cyber ability and force.

Therefore, here the cyber domain plays a unique role. Cyber capabilities in themselves have so far not caused direct armed conflict, which has allowed some states to take greater risks in their

engagement with one another. However, there are counterarguments on the conduct of responsible states and how cyber capabilities should be deployed (Saltzman, 2013). Thus, states might adopt increasingly offensive posturing against one another and, in the present political state, not be caught in a rapidly escalating cycle leading to armed conflict. Concurrently, as warfare becomes ever more entwined and reliant upon cyber capabilities, the ability to shape battlefields through cyber means become ever more important, to the level where they may affect kinetic warfare operations. The weakness here is that the messaging may already be considered turgid and the credibility of offensive comments undermined (Hanson & Uren, 2018).

Nonetheless, a viable counteroffensive or punishment strategy is required, even if just as part of cyber-conflict resolution and normative expectations. The ASD, AFP and ADF comprise offensive cyber capabilities and regularly make public assertions on capability and readiness training, with the Defence Cyber Security Strategy 2022 clearly outlining that 'defence must continue to improve its cyber-security if it is to defend against constant malicious cyber activity and succeed in future conflicts' (Department of Defence, 2022, p. 7; Garman in Bagley, 2023). So cutting-edge capabilities are seen as a requisite for mission success. Importantly, the 2022 strategy clearly stipulates that cyber has emerged as a warfighting domain, that denial is not always a viable strategy and that the information realm will also be a critical component of future conflict as part of a commitment to an Australian grand strategy (Department of Defence, 2022, p. 8).

Entities such as the Defence Science and Technology Group (2023) also have multiple cyber divisions to support the DSTG's overall mission as being the 'lead agency responsible for applying science and technology to safeguard Australia and its national interests' (Defence Science and Technology Group, 2023). This includes a specific cyberwarfare operations branch of the Cyber and Electronic Warfare Division, which

> undertakes the research and development of new and novel concepts, technologies and techniques in order to enable autonomous, resilient and effective cyber capabilities with an operational edge in the face of ubiquitous encryption, untrustworthy ICT and a highly dynamic and sophisticated threat environment. (Defence Science and Technology Group, Cyberwarfare Operations, 2023)

Ultimately, the ADF has multiple assets and divisions that are devoted to not only deploying offensive cyber operations but also researching and developing their own suite of advanced capabilities to suit them, commensurate with mission success in operational terms.

Communication is an intriguing part of a deterrence-by-punishment strategy in the cyber domain while pointing to the necessary to have comparable assets to punish to help to prevent escalation. Hence, Australia should always attempt to pursue suitable dialogue with China on deterrence signalling, crisis management and normative expectations. Furthermore, attribution still matters a great deal for threats of punishment. As discussed earlier in the thesis, the Australian Government was initially hesitant to specifically identify China as an antagonist state (Packham, 2019), but its geopolitical and political practices appear to have changed. This 'name and shame' approach can be seen a significant communication development for Australia in itself (see M Payne et al.2021). Equally important is the combined efforts of attribution Australia has made with its allies, as discussed in Chapter 4. These combined efforts can be seen as signalling resilience and capability to the China, as well as adhering to Libicki's (2009) deterrence framework to better respond to what matters.

5.6 A Deploy Payload Blueprint: Destroy, Disrupt and Degrade Target Chinese Networks

Offensive cyber operations conducted without context and within a poor analytic framework will, in effect, be an aimless and counterproductive coercive gesture that may not satisfy political and strategic objectives, including that effective signalling should be clear and specific.

Cyber operations can have large opportunity costs and retaliatory operations should be conducted with specific strategic objectives in place or there is a significant risk for escalation if the aggressor does not understand the reason it has been hit. As stated, timing is of the essence in the cyber domain and in deterrence-by-punishment thinking. If an aggressor such as China cannot link an act of retribution to its own initial conduct, or if it rejects the evidence provided to it in the handling of the crisis (i.e. insufficient attribution), then deterrence by punishment should be considered ineffective and potentially escalatory. The relational variable discussed in Chapter 1, the sliding scale on the effectiveness of deterrence, slides ever further towards ineffectiveness as the temporal continuity and contingency between acts of aggression and retribution extends. It is completely nullified by ineffective attribution.

Therefore, contextualising an act of cyber retribution within a deterrence framework will greatly assist the viability and sustainability of deterrence-by-punishment approaches. In Chapter 1, the three most consistent aspects of a deterrence strategy were introduced: political credibility, including the will to deploy deterrent mechanisms despite potential blowback or escalation; technical capability; and clear communication, in efforts to deter and respond to serious cyber incidents. Breaking down these three factors will inform the analysis of Libicki's (2009) punishment framework.

A first question that must be answered is what options are available for retribution within the context of strategic cyberwar—framing that must also treat cybersecurity as a genuine whole-of-nation undertaking. Here, the case study of Estonia in 2007 provides crucial context for much of the prior discussion as well as Australia's future ability to operate, innovate and disrupt against an actor such as China.

In 2007, Estonian web services came under sustained attack most often via DDoS attacks, which, put simply, is to overwhelm the bandwidth of a website and cause it to crash. The ramifications were the disruption of banking services and governmental websites, and more than 100 websites were affected (Greenberg, 2019). The attacks were eventually attributed to Russia-based attackers by forensically tracking the botnets conducting the DDoS operations and through operational and strategic analysis, lending to the attribution and the conclusion that they were launched from a Russia-based IP address (McGuiness, 2017). A key consideration was that the attacks began almost immediately after the Estonian Government decided to move the Bronze Soldier from the centre of Tallinn to a military cemetery on the outskirts of the city (McGuiness, 2017). A quick breakdown of events highlights how deterrence by punishment can be considered by states such as Australia and is also illustrative of its difficulty.

Significantly, ambiguity was a defining feature of this cyber attack:

> As the attacks were apparently carried out independently by individuals using their own resources, any state sponsor responsible for orchestrating the attack was able to disguise and deny themselves as the source. This underscores the requirement for governments to achieve political consensus on attribution in a timely manner based on the available evidence and be able to communicate this in a clear and understandable way to the general public. (Pamment et al., 2019)

Nonetheless, attribution was conducted by Estonia and was seen as sufficiently compelling to go public with the accusation that Russia-based patriot hackers were behind the incident, but informally, unnamed sources alleged that the Kremlin had initially orchestrated the attack and it was then picked up by 'malicious gangs' (McGuinnes, 2017). The vast majority of malicious network traffic was of Russian-language origin and

> had indications of political motivation. The Russian government denied any involvement; however, the cyber-attacks were accompanied by hostile political rhetoric by Russian officials, unfriendly economic measures, and refusal to cooperate with the Estonian investigation in the aftermath of the attacks, all of which likely encouraged the perpetrators (Pamment et al., 2019).

The operations can be seen as part of a strategic cyberwarfare attempt as the computer network attacks targeted the functions of the Estonian State. The context fits Libicki's strategic cyberwarfare definition and also answers the attribution question. Accordingly, Estonia is now in a position in which it must consider how to best respond to the aggression. Deterrence-by-denial efforts have obviously failed: Does it turn now to deterrence by punishment as part of a multilayered deterrence mode? Is there a retaliatory action in the cyber domain that Estonia can carry out that does not risk escalation or send the wrong message to their allies? Further, can they hold the assets of the cybercriminals at risk, and can they do so repeatedly? Will third parties join the fight, given that Estonia campaigned that it was a violation of NATO's Article 5? (Herzog, 2011).

In terms of the last questions, it is worth noting that collective self-defence was not automatically extended: 'Not a single NATO defence minister would define a cyber-attack as a clear military action at present' (Traynor, 2007). Despite this, the current belief is that the actions of pro-Russian hackers were conducted at the will of the Kremlin, but despite various data points about the attacks coming from Russia itself, there was not enough data for Estonia to publicly blame the Russian Government itself, or at least not enough for Estonia to comfortably do so and absorb the potential diplomatic repercussions of such attribution (Barnes & Sanger, 2020). The situation eventually diffused over time, in what Libicki (2009) describes as a return to the 'muffled din' that preceded cyberwarfare wherein the associated operations receded over time while the event demonstrated the complexities of such warfare (p. 136).

At the time of these attacks, others also expressed concerns that without clear global norms and expectations around cyber offences, including a target's rights in terms of deterrence-by-

punishment actions, such attacks will only regenerate. Cyber-policy expert Melissa Hathaway argued that that the lack of strong, predictable responses to cyber attacks is contributing to 'a new de facto norm — 'anything goes' — and this is dangerous because it increases the risks to international peace, security and stability' (Maclellan & Oleary, 2017). Rebecca Crootof added that 'states are likely to have delayed reactions to cyber-operations — and delayed reactions look more like prohibited punishment than permissible countermeasures' (Maclellan & Oleary, 2017).

Importantly, this also refers to the attribution situation outlined above—attribution does not have to be specific rather than speculative to begin discussions of countermeasures and potentially retribution—with a focus on a credible, timely responses. Simultaneously, a key problem was that the cyber operations did not produce permanent physical damage to property or citizens to Estonia, meaning that it fell short of armed violence thresholds. Liisa Past pointed out that 'Cyber aggression is very different to kinetic warfare … it allows you to create confusion, while staying well below the threshold of an armed attack' (McGuiness, 2017).

This is informative for Australia in its considerations for a deterrence-by-punishment strategy against China. This will incorporate not only efforts to make its data and related Australian digital systems as resilient as possible to mitigate or prevent disruption but to convince China that their prospective gains from attacking Australia will not be worth the effort they must expend. These threats of serious consequences will then be part of a larger strategic gamble that aims to avoid setting off an escalatory cycle; thus, implementing punishment practices will again need to be timely, credible and proportionate. The cyber domain also has a levelling effect in power relations—states smaller in stature can now compete with larger states as long as the arena of contest is limited to the cyber domain. Libicki 92009) also made a strong point that in the cyber domain, supremacy is impossible when compared with the supremacy of air, land or sea warfare (p. 141). The relevance is also that capability to carry out deterrence-by-punishment mechanisms is at the discretion of the executive in the Australian Government with a focus on cybersecurity and multi-nation strategies. Even if facing difficult-to-attribute cyberthreats, cyberwarfare capabilities can still be signalled and commutated to actors such as China. However, one reality remains the same and may have influenced Estonian actions, including public attribution, namely, that power relations and diplomatic relations remain the same despite the levelling effect of the cyber domain. Hence, Australian decision-makers would still need to be considerate, as the Estonians possibly were, that escalation out of the

cyber domain is undesirable, and the benefit of retribution over nothing would need to be carefully considered.

Further, the seriousness of the cyber attacks on Estonia generated a rapid international response. Furthermore, punishment options received fairly widespread international support, including from the European Union, the US and NATO (Herzog, 2011). Thus, while it is important to develop independent capacity to carry out deterrence operations, Australia also has a track record in recent history of multi-nation public attribution and collective measures throughout multiple governments in coordinating public diplomatic and legal responses to malicious cyber activity conducted by Chinese entities. For instance, as mentioned in Chapter 2, Australia was among many of the countries in 2021, including the US and the UK, that publicly attributed and blamed China for malicious cyber activities that had attempted to exploit vulnerabilities in the Microsoft Exchange software (Hurst, 2021).

Therefore, while China uses cyber attacks below the threshold of war, Australia has still continued to devote significant energy, time and investment in developing not only its own cyberwarfare capability but also its relationships to enhance its ability to enlist third parties in the fight. Redrup (2020) and others have even argued that Australia's position 'as a leader of the Five Eyes is firming up, with proposed amendments to the Security and Critical Infrastructure Act giving the Australian Signals Directorate "step-in" powers that cyber experts say put it at the front of the pack'. This may be inferred as the development of political capability, as in its Five Eyes membership on cyber subjects of mutual interest and concern, alongside a growing technical capacity to conduct deterrence-by-punishment operations and the pursuit of related national goals. For instance, in 2023, the Five Eyes alliance discussed the topic of 'zero-trust' architecture and networks. A zero-trust network is a security model 'in which it is assumed that no party is verified or can be trusted at any point, meaning everyone and everything must be verified continuously for access to be granted' (Croft, 2023). The continuation of these discussions is a public messaging of a technical uplift in capability across Five Eyes partners and the inference of shared capability and shared responses to cyber incidents.

At times, technical capacity in Australia has puzzled decision-makers as specificity on what cyberwarfare can achieve has been difficult to determine. This makes Libicki's (2009) definition of strategic cyberwarfare so useful—once the state is stipulated as the victim of computer network attacks, then the range of actions that deterrence by punishment needs to

respond to narrows down (p. 117). A narrowing the range of options reduces the demands on the said victim state to develop its own cyber capabilities, and thus, the inference that the cyber domain is a levelling situation between powers is ever more enforced. Constraining the range of attacks within computer network attacks as the defining factor of cyberwarfare and removing computer network espionage (CNE) from the equation removes a significant portion of malicious cyber activities and can make decision-making much clearer and credible when considering deterrence by punishment.

In fact, Libicki (2009) gave important structure on this consideration, asserting that 'any self-respecting military should expect to be the target of state-sponsored CNE at all times' (p. 141). Espionage, and by default CNE, is a legitimate state craft and is something that all states engage in (Besser & Sturmer, 2016). Hence, a computer network attack is a useful threshold for cyberwarfare, and states being the victim is a useful metric for asserting that strategic cyberwarfare has taken place. Once these considerations are acknowledged at the political level, the technical capacity consideration is simplified to the question of intended damage and the impact and implications of any collateral damage.

In terms of the damage that Australia can inflict in the cyber domain on an aggressor state, ultimately, the specific answer to this question is a confluence between what Australia can technically execute and what policymakers are willing to execute, including all cyber activity that falls below the level of armed conflict. As has been outlined in prior chapters, Australia has emphasised the development of cyber capabilities and, significantly, has put organisations such as the ASD on platform where a good defence will also mean a good offence. The implication is that punitive cyber operations are now an option available to the government to put pressure on the threat but presumably as an option that is considered after diplomatic options are exhausted or considered infeasible.

Libicki (2009) also acknowledged this in this punishment framework, stating that *sub rosa* cyberwarfare may be preferable, since elevating such incidents completely to the public eye may be seen as escalation by the antagonistic state and potentially cause a tit-for-tat exchange that does not stop (p. 128). However, it also remains to be seen what actions in the cyber domain would actually lead to kinetic conflict since no such non-cyber confrontation or war has been carried out as yet. Therefore, when carrying out acts of retribution, there is still a broad threshold that these actions can operate within certain normative standards and should be

considered viable by a decision-maker in seeking to punish poor conduct, which would prove their actions are timely, credible and proportionate.

5.7 Punishment Frameworks and What Was the Original Purpose of the Attack?

As an element of any timely, credible and proportionate punishment framework, before deploying a retributive payload, Australia should consider a direct warning and always consider the intentions and motivations of the aggressor who has conducted the malicious cyber attack. This might incorporate efforts to gain a better situational awareness and to share further information with allies. 'We want to normalise cyber capabilities and should treat them like any other military system, rather than as dark secrets from the world of SIGINT' (Lewis, 2016). The flip side of this approach is that in the case of cyber assets, it is difficult to find scenarios comparable to the regular use of military assets—for instance, it is unclear what cyber operations would constitute something like a Freedom of Navigation exercise that the Royal Australia Navy has conducted alongside the US, much to the protest of the Chinese (Panda, 2017). These exercises are clear displays of power and intent but were not escalatory enough to trigger the onset of war. Normalising cyber capabilities in this sense would be useful for Australia in deploying retributive cyber actions.

Strategic thinking on escalation will become ever more crucial as states continue to invest in the development of cyber weapons that can create massive follow-on but unintended damage, such as WannaCry and NotPetya (Fier, 2019). Consequently, Australian decision-makers need to be careful in their own cost–benefit analysis, and the ASD, AFP and Defence will need to work together in a cooperative manner in determining attribution and, potentially, the intention of an attack, given that threats can manifest in various ways. Of course, part of the review must also involve an investigation of the denial defences—good defences should help to filter out third-party attacks and isolate network penetrations to deliberate efforts (Libicki, 2009, p. 73). Unfortunately, what should happen and what happens in reality are often not the same; therefore, this assessment will be necessary in contextualising retributive actions.

As discussed throughout the thesis, China is prolific in CNE activities and much of its cyber operations are described as 'rob, replicate and replace'. Presumably, if China is observed conducting CNE that entails pilfering intellectual property, this is not an action that would be considered a direct attack on the state or the conduct of strategic cyberwarfare with associated

military operations. However, if state systems or civilians and their properties are damaged by cyber incidents, Australia may interpret this as deliberately harmful and escalate matters. Such unintended flow-on errors speak to the difficulty of assessing the intent of the cyber attack itself: Did the aggressor state just make a mistake or miscalculation or other? Therefore, it will be valuable to conduct further research on the unintended effects (or game theory) as well as the role of the principle of proportionality in the more ambiguous 'grey zone'.

Such an analysis might also provide more clarity on the application of norms in the context of cyber attacks. Nevertheless, assuming that error has been ruled out and the attack has deliberate denial and manipulation effects, offensive cyber operations may be integrated into policy planning. Herr and Rosenzweig (2014) defined such cyber weapons as malware that has a destructive digital or physical effect. Others have also described two forms of coercion: active coercion (or compellence) and passive coercion (or deterrence):

> The former involves the active use of force in some form to compel action by another, while the latter involves the threatened use of force to motivate an action or restraint from an action. In reality, the distinction is more of a continuum, as some states may combine compellence actions with the threat of more devastating consequences to accomplish their ends. (Hodgson, 2018, p. 74)

Therefore, coercion in the cyber domain is very difficult to apply without context and without understanding the nature of specific state-to-state relations (Hollis, 2010)—in this instance, the China–Australia dynamic, as explored in pervious chapters. While the promise of cyber coercion will always exist, a coercive measure might be methodical albeit non-explicit as to not allow an actor such as China the opportunity to pre-empt the action.

Alternatively, an aspect that makes the explicit threat of punishment challenging is that if the threat is too peculiar and detailed, then China might simply prepare its defences, which may nullify the attempted coercion. Given that Australia (and its allies) can be expected to continue to pursue coercive actions through cyberspace, indirect or non-explicit coercion is a possible policy action, with the aim of seeing a change in behaviour by the coerced. For instance, when NSA engineers discovered a vulnerability in the Windows operating system, rather than remaining silent, the agency notified Microsoft and then went public about the impact and intention, in part, to improve resilience (Nakashima, 2020). But this public statement of capability can be part of indirect coercion, as the NSA was showcasing its technical abilities, gaining international consensus on the issue and asserting detection and response capabilities.

A paranoid mind could also argue that the NSA was only willing to divulge its understanding of said vulnerability after it had drained the vulnerability of its usefulness or observed adversary states such as China utilising it themselves. Given that an explicit threshold for coercive response was not stated, it can be argued coercion still occurred in a context of significant ambiguity. Thus, overall, an effective deterrence-by-punishment strategy must use

> communications, messaging, and signals with opponents, allies, and publics. This does not mean that every action should be accompanied by a press release, but a new cyber strategy will need to use public and private communications to shape opinion in ways favourable … and make it clear that our actions are guided by international law and agreement. Adopting a more assertive posture in cyberspace is in itself a message that will improve position with opponents. (Lewis, 2022)

Of course, building and maintaining alliances and communicating with the Australian public as well as China will require addressing issues of evidence and attribution, as discussed in Chapter 2, about the publication of Chinese campaigns by the ACSC, and in Chapter 4. The strategy should also consider cyber operations that appear intended to make 'an otherwise infeasible military attack can be made feasible by a bolt from the blue' (Libicki, 2009, p. 82), that is, operations from China that may presage an assault on Taiwan. This type of conflict is more reliant on conventional military actions, while operational thresholds under this more extreme type of umbrella of force will attempt to damage or destroy military capabilities or disrupt command and control and related strategic military capabilities (Ryseff, 2017). The challenge for Australia and a deterrence-by-punishment strategy is that it considers not only the defence of Australia itself but also prosecutes Australia's interests in the region, which is the desire for a stable and peaceful cyberspace and Indo-Pacific region (Watts, 2023).

5.8 Unpacking the Punishment Framework

The definition of force in cyberspace is problematical. Nonetheless, the Australia–China relationship in cyberspace has been contextualised, and the context of retribution and how it functions in the cyber domain have been discussed. This next section will be devoted to unpacking Libicki's (2009) framework question by question in the event of Australia discovering that it has been the victim of a deliberate strategic cyber attack by China. Assuming that denial actions have proven inadequate, deterrence by punishment is possible but still fraught with difficulties and a number of questions, as guided by Libicki.

5.8.1 Can We Hold Their Assets at Risk?

This particular question receives greater focus owing to the nature of the cyber domain, how assets are managed, how they are made vulnerable and then invulnerable, and the mercurial nature of how they exist. Assets in the cyber domain can be vulnerable because they are poorly patched, but subsequently hardened immediately from said patch; default settings are changed; and there is separation of networks from being public facing to hiding behind Virtual Local Area Network; the list of such defences goes on (Libicki, 2009, p. 83). The question of how to hold assets at risk, and persistently, is a significant conundrum.

The first difficulty of this question is identifying the assets that, at a minimum, might cause temporary disruptions. The first consideration of the Australian Government in this scenario is deliberating on the target that it must hit in return that would cause sufficient cost to the attacker and eclipse the benefits of their initial attack (Gilding, 2020). In a deterrence-by-denial scenario, this would be realised in that the efforts the attacker must go through to conduct the attack are greater than the pay-off of the attack itself. In punishment, the retribution must be greater than the benefits of the initial attack. Proportionate response becomes critical in this question as the Australian Government would not want to risk landing a disproportionate blow in response to what was a minor infringement, or worse, as explained earlier, actually a mistake or miscalculation.

For more context, there are unique conditions to cyber operations. Cyberwarfare is reliant on intelligence—the battlefield must be readily prepared for offensive cyber operations to take place as it involves the search for vulnerabilities in specific systems that can be exploited in specific ways (Libicki, 2009, p. 155). Then, these vulnerabilities are what become weaponised and direct cyberwarfare to take place below the threshold of an armed attack (Gilding, 2020).

The purpose of this elucidation is to clarify that vulnerabilities must already be known and somehow held in readiness should a strategic cyber attack be discovered, and should be attributed quickly and credibly so that deterrence by punishment appears in response to the specific incident. Regarding the key role of the principle of proportionality, decision-makers in Australia should also focus on determining the effects they would desire in response to certain cyber incidents. By organising responses into effects, decisions could potentially be made faster to deploy specific payloads that would hopefully be able to satisfy these demands. These effects could be communicated in non-explicit ways while managing the risks of

unintended escalation. Lonergan and Lonergan (2022) added that cyber operations can act as ‘accommodative signalling under some conditions, particularly when decision makers are faced with managing tensions between simultaneously signalling to domestic audiences and adversary governments’ (p. 33). In essence, offensive cyber operations do not necessarily need to be successful, that is, destructive, but could be beneficial simply by the fact they are known, signalling a state’s displeasure by virtue of existence.

First, Australia has shown that it has significant attribution capabilities, even declassifying some past operations that revealed both advanced attribution skills and well-suited teamwork with allies, as discussed in Chapter 2 (Borys, 2019). At the very least, it may be inferred that Australia has the technical capacity to hold Chinese assets at risk although it remains unclear whether its actions will always generate the desired effects, especially if they are not proportionate.

Second, what particular assets are held at risk would determine how often they could be struck. In broad terms, deterrence of more destructive attacks is an obvious goal for Australia. Being able to repeat effects mitigates the capacity of the actor facing retribution to, in turn, simply mitigate or absorb punishment. It also would affect the targets’ strategic thinking: If the same effect is being replicated across multiple networks and systems, how secure are the rest of their defences? In fact, replicating effects across a spectrum of systems may have a greater impact on the strategic thinking of a state, including China, than simply hitting a target once. Of course, this is easier said than done, as replicating effects would involve reasonably similar vulnerabilities; once the vulnerability that generates an effect is discovered, then similar results may be hunted for across the spectrum of equipment. Consequently, a significant limitation for Australia is that the punishment effort would require a sophisticated understanding of a broad range of China’s cyber landscape and also have the understanding to exploit a multitude of vulnerabilities across a spectrum of its assets and equipment. This is a monumental task and there is little to no indication in open-source literature that the Australia has this type of capacity. Libicki (2009) made it clear that retaliation cannot sublimate an attack, particularly attacks that take on the nature of botnets or other such attacks that are essentially diffused over enormous numbers of computers (p. 60).

Third, a likely consideration for the Australian Government is whether it should decide to call upon the US and the Five Eyes or associated groupings to assist in retribution against Chinese cyber operations. Concurrently, Australia’s inclusion of third parties may possibly stimulate

China's inclusion of third parties—the PLA, SSF, MSS are not the only cyber operators in China, and the phenomenon of patriot hackers in acts such as espionage must also be considered. Indeed, contesting states may resolve their issues *sub rosa*, but actors such as patriot hackers are potentially unaware or uncaring (Libicki, 2009, p. 63). Therefore, Australia's capacity to avoid the escalation of a cyber conflict might also depend on its ability to stop patriotic hackers (or proxies) from continuing or even intensifying the conflict.

Hence, while Australia might be better served in terms of impact by developing and acquiring offensive capabilities in tandem with allies, the recruitment of third parties may also trigger escalation from the aggressor state (or proxies), which means that deterrence has failed. Simultaneously, collective security measures can convey attribution and displeasure without committing kinetic resources to limit tensions from spilling over. To date, even the ANZUS Treaty itself has been invoked once, by the former Howard Government as part of Australia's response to the 9/11 terrorist attacks (Hartcher, 2022). Asked whether Australia could invoke ANZUS in response to a cyber attack, in 2022, Anne Neuberger, the cybersecurity advisor to President Joe Biden, stated:

> the partnership between the US and Australia on intelligence and cybersecurity is so deep that we would expect that if there was any significant cyber-attack, whether in Australia or the US, we would each be there for the other in terms of rapid intelligence sharing, rapid incident response and remediation, and then determining attribution and consequences (Hartcher, 2022).

At present, such a wording captures ambiguity in terms of effects, sources and commitments, although it also does signal a level of common third-party agreement in a more strategic and operational sense. Other examples would be the partnership between NATO and Estonia in 2007 although the cyber attacks did not trigger Article 5 (Stotenberg, 2019). The involvement of patriot hackers also muddied the waters on attribution.

Fourth, Libicki (2009) discussed how if private companies operating within the victim state (e.g. Australia) are aware of a deterrence strategy, they may be less inclined to protect their systems as they can offload responsibility and subsequently costs to the host state (pp. 64–65). However, as discussed earlier, retributive action may be best conducted *sub rosa* and the private institutions within Australia be none the wiser that there was any response on their behalf. For the most part, the Australian Government can operate on a need-to-know basis for private companies operating on its infrastructure and can also insist that these companies be

vigilant in their own security should they desire the privilege of running services such as electricity.

Fifth, precise thresholds for response are difficult to define. Strictly speaking, anything that leaves systems functioning in an unintended way could be used to justify some form of retaliation (Libicki, 2009, p. 65). However, a zero-tolerance policy is unwise as deterrence strategy is legitimised by credible and proportionate action: What if the only consistent action is that the victim state does nothing as they are incapable of detecting sophisticated intrusions? This consideration bears further relevance from Australia's 2017 strategy asserting that Australia has the right to do nothing if the state so wishes (Department of Home Affairs, 2017, p. 26). What if they can only partly detect malicious cyber activities? Intermittent retaliation does not necessarily cause an attacker to take pause; instead, they may be astonished at why they suffered retaliation now and not before (Libicki, 2009, p. 66).

In short, small-scale attacks that produce limited effects are unlikely to justify retaliation, provided Australia is interested in proportionality. A zero-tolerance policy does communicate resolve in retaliation at least, and that the victim state will return fire when provoked. The issue is that Australia has already stated its position, or at least what it is not. By not naming and shaming the state that perpetrated the hack of political parties discussed earlier, the Australian Government signalled that its deterrence position is at least not zero-tolerance and that it will tolerate some cyber attacks, at least publicly. Furthermore, with the proliferation of the naming and shaming of China, Australia has been informally describing thresholds of unacceptable action from China (as discussed in Chapter 2). At the least, communication channels between Australia and China must be well constructed and recurrently available.

As stated earlier, rather than focusing on the actual potential targets that could be hit themselves, it may behove the Australian Government to focus instead on desired effects. These effects may be ordered into separate thresholds that can limit actions and hopefully prevent escalation. Using the 'missile down your smokestack' scenario presented earlier, the reasonable assertion is that disabling electric power grids for significant periods of time or scale is a threshold that should not be crossed. Conversely, penetration of certain functions of the Australian Federal Government (political parties) *will* be suffered but not be appreciated. Effectively, CNE is a tolerated cyber attack for Australia even if, in certain circumstances, it will make public the CNE and rebuke the actors involved.

Last, as stated, offensive operations do carry risks. Ambiguity can be both an asset and a liability, even if responding in a non-public manner in order to make it easier for the other side to de-escalate. As Axelrod (2017) revealed:

> In kinetic warfare, there is a widely shared sense of what counts as escalation and de-escalation. For example, the use of a nuclear weapon would be seen by all parties as a very large jump in the escalation of combat. In contrast, cyber conflict has no such clear breaks in its escalation ladder. Even more importantly, two adversaries may have very different conceptions of what counts as a significant escalation, and therefore what cessation of activity would count as a significant de-escalation (p. 2).

It is important to note from the above quotation that a large portion of what determines unacceptable in the cyber domain is the risk appetite of each entity, and that distinct entities such as Australia and China likely have different risk appetites. Escalation in kinetic warfare operations can be conceptualised by the weaponry at the state's disposal and the effects they will generate. Hence, reducing the level or scope of deterrence-by-punishment activities might be the most uncomplicated method of avoiding the escalation of a cyber conflict. In cyberwarfare, simply because effects are desired does not mean they are necessarily available in operational terms. As stated above, cyberwar attacks rely mostly on discovered vulnerabilities: What if the only vulnerabilities exposed are disproportionate and would invite escalation? A principal consideration for a state such as Australia would be to arrange the effects desired and overlap these on the vulnerabilities exposed, and subsequently decide whether sufficient options are available in the cyber domain to achieve these effects. For Australia to avoid escalating the situation, it would require the holding of specific assets at risk for the purpose of responding to specific cyber attacks that are at least proportionate.

One particular challenge would be identifying the point at which Australia can threaten critical infrastructure with cyber attacks. Can Australia make such a threat—cyber weapons require networks to be accessible, for a vulnerability to be identified in the target system and a weapon tailored around it, and then the payload to be received and triggered on the target network before it hopefully unleashes its damage. If these conditions are not satisfied, then the ability to unleash this form of punishment is denied and is potentially counterproductive (Lonergan, 2017, p. 5).

Would such a costly signal of threat even be taken seriously by China? At present, there is little reason to expect Australia to publicly make such an explicit threat (Wroe, 2019). However,

with the onset of 5G internet capability, threatening critical infrastructure seems much more dangerous than before on 4G networks, especially given the unpredictable effects of cyber weapons (N McKenzie & Galloway, 2020). Uncertain effects must be closely considered by victims of offensive cyber operations as well as the aggressors who conduct these—the capacity for error or miscalculation incidents, as discussed earlier, may have far greater ramifications in future because of the mass connectivity of 5G networks (which may, in turn, greatly amplify possibilities for escalation). This also demonstrates an inherent difficulty that the cyber domain has that other warfighting domains do not, at least not to the same capacity in undertaking preparations. Cyber incidents can evolve because an individual has made an inadvertent mistake, which would therefore not be justifiable in term of punishment and offensive retaliatory policy actions.

5.8.2 Assessment

Punishment responses to cyber attacks will require a nuanced and tailored response. Certainly, deterrence by punishment does provide a viable strategy for Australia. However, Libicki's (2009) framework begins first and foremost with advising caution. At almost every level, retaliation in the cyber domain is fraught with difficulty not only at the technical level in the form of attribution but also at operational and strategic levels. Hence, Australia's commitment to capability building and credibility should be reflected in policy and proposals aimed at directing future cyber operations build-ups.

Further, the capacity of cyber incidents to be poorly interpreted cannot be overstated. CNEs that results in error incidents are not only possible but also quite likely, and it has been established that cyber attacks are reliant on intelligence gathering through various means first and foremost to discover a vulnerability (National Cyber Security Centre, 2021). This reality may not be reassuring, but it is instructive that a damaging cyber incident may have simply occurred because an antagonistic state was investigating the potential vulnerability. The attribution problem is not only the forensic collection of data after a cyber attack has been detected but also the strategic consideration of the opponent's intent, what they might have been trying to achieve—and identifying whether this did, in fact, have inappropriate intent, such as undermining national command authority.

Once the attribution and intent problem is satisfied, many other issues may arise. What retributive effects can the victim state even put into play against the antagonist, and are these

still proportionate? Can they be replicated? Does the victim even *want* to commit retribution, acknowledging that their networks were penetrated and it has infuriated the victim enough that they would lash out?

The ramifications here are that Australia will at least take some sort of action in the public arena against China or related entities. Further, while the Chinese Government has expressed disappointment and discrimination in various cyber-related matters, it also appears that the Chinese Government for its part accepts some degree of blowback for its malicious activities (Berman, Maizland, & Chatzky, 2023).

However, what is not instructive about an issue such as the Huawei ban, for example—Australia was the first country to ban China from its 5G network—is where thresholds truly begin to take shape (Hartcher, 2022). Concurrently, banning Huawei from developing 5G networks in Australia is not the same as undertaking cyberwarfare operations. Nonetheless, it can be argued that the issue of escalation is perhaps the most difficult to overcome, and having a disproportionate response at one's disposal is not only expensive, unethical, illegal and difficult to politically obtain, but the said vulnerabilities may be patched and rendered useless anyway. Yet, if the punishment response is so simple, woeful or limited, then the antagonist might not even notice and will continue their misconduct oblivious to complaints and (inconspicuous) punishment actions.

5.9 Conclusion

Cyber attacks against Australia will affect and shape the conventional strategic calculus. The attribution and communication problem might also introduce an amount of uncertainty, complicating decision-making.

In terms of deterrence punishment actions, Australia should not refrain from retaliating all the time—for that would raise doubts about its punishment capacity—and it should not respond all of the time—as that could be disproportionate and could lead to unintended escalation. The best policy realignment would be to retaliate some of the time, even in a randomly albeit timely fashion, after assessing issues such as risk of clarity and certainty of punishment. Crucially, at the same time, the severity aspect of a punishment should be connected to the level of aggressor damage, impact and motivation, wherever possible.

Chapter 6: Conclusion and Discussion

6.1 The Research Question

As stated in Chapter 1, the core thesis question was ‘Is Cyber Deterrence by Punishment possible? Furthermore, can Libicki’s (2009) deterrence-by-punishment strategy assist Australia in deterring Chinese cyber aggression?

Cyber deterrence is a quintessential security concept that differs from traditional deterrence thinking. The primary strength of utilising cyber deterrence—by denial and/or by punishment—in the cyber domain is that Australia can feasibly contend with China on a holistic and strategic basis. Further, attribution is possible (Chapter 4), and Australia has invested heavily in policy efforts to influence China’s behaviour by discouraging it from engaging in unwanted and malicious cyber activities such as hacking (Chapter 2). In particular, the ASD is a key government body to detect increased threats and respond to incident data, and it continues to maintain a high level of advice and expertise in supporting cyber capabilities, thus forming the key component of offensive cyber operations (Scott, 2023).

Denying benefits and imposing costs as a feasible practical security solution in a multi-domain world has also taken place in a particular political and diplomatic context and has incorporated key elements such as signalling and communication, as evident in Australia’s decision to deliberately ‘name and shame’ China since 2018. A perfect system of deterrence in the cyber realm is impossible since there will always be some sort of avenue in cyberspace to exploit, but such signalling is an attempt to set clear expectations for state behaviour in cyberspace. In particular, such ‘red lines’ can set the tone of, and help to direct, deterrence by punishment policies in the cyber domain (Chapter 5) albeit not without challenges, including the dangers of unintended escalation.

This framing lends to a strength for Libicki’s framework as well, which also carefully considers unintended escalation as well as the involvement of third parties, such as the cyber provisions added to the ANZUS Treaty in 2011. In this regard, alliance and partnerships with third parties also imply improved capability for Australia because its partner states, such as New Zealand, the US, Canada and the UK, can all assist Australia in deterrence by offering capability or intelligence on Chinese systems and networks that Australia could then exploit. Such risk

reduction measures can also be interpreted as efforts by Australia to build confidence in any partner state's capacity to collaborate in response to cyber incidents.

Libicki (2009) provided a cogent framework for considering how deterrence may be conducted, with a blow-by-blow analysis lending the decision-maker an interesting model to consider (p. 39). This thesis has contextualised Libicki's framework, applying it for Australia deterring China, and has asserted that although fraught with some difficulties, the framework offers a firm foundation to enable a pragmatic range of response options. In particular, the defence of critical infrastructure is imperative as digital networks proliferate, and cyber deterrence itself will become increasingly important to deter and respond to unacceptable behaviour. At the same time, China will remain a central security concern, and as highlighted in Chapter 3, it has been involved in multi-year cyber espionage and related campaigns and has embraced new forms of cyber-enabled warfare.

It is essential that Australia employ all policy options available to it to ensure the defence of national interests, including critical infrastructure, in the backdrop of strategic competition, albeit some questions remain over the measure of realistic deterrence expectations regarding 'sophisticated' attacks (from both a public and government perspective), or the unique characteristics of REDSPICE and how this programme will enhance Australia's deterrence capabilities and capacity to meet said realistic deterrence expectations. In this sense, more could be done to better categorise different types of cyber attacks publicly in order to better identify appropriate and proportionate retaliatory responses.

Nonetheless, attribution will entail both political and technical dimensions and can have a variety of policy outcomes. For example, precision attribution can remain the province of criminal prosecution, whereas 'confident attribution' can satisfy the retributive thresholds of a state against another state that does not need to provide a compelling case before a court. Further, owing to the hidden nature of the cyber domain, it is possible that the international community is not even aware of the type of cyber attack that has occurred, and states can have these non-kinetic interchanges 'quietly' and possibly without raising concerns among others. Escalation is still a significant issue and must be balanced with the idea that the punishment exacted must be credible, however, and states will still benefit from extracting precision attribution in the event that a quiet non-kinetic interchange suddenly becomes public (and therefore involve 3rd parties wanting evidence).

As discussed in previous chapters, determining the appropriate level of retaliation will remain highly important in developing a credible policy. Further, vulnerabilities need to be known and be readily exploitable. These vulnerabilities also need to be, as stated, proportionate to the alleged incident. For instance, amassing botnets and potentially launching DDoS attacks on websites are not useless but do not carry much power on a national or strategic level. Therefore, any cyber penalties to be addressed will need to consider the motivational calculus of China. That is, the scale and type of response to a cyber incident that might impact the cost–benefit calculations of Chinese policymakers (or proxies) and change their behaviour in cyberspace to Australia's advantage should be ascertained. Moreover, as argued, China has been made aware that Australia can inflict significant damage in cyberspace but also does not want a defensive or more likely offensive posture to unintentionally escalate a situation. Overall, the concept of deterrence is highly relevant and applicable to the cyber domain, especially in its ability to influence the strategic calculus, in both political and psychological terms, of actors such as China.

6.2 Contribution to Knowledge: Conceptualising Cybersecurity and Risk Strategy

Given this discussion, it can be argued that cybersecurity is essentially about managing risk (Yao & de Soto, 2022). Further, policymakers must carefully consider credibility, communication and capability components in matters pertaining to national cybersecurity issues. Furthermore, punishment by its nature cannot drive down the risk of consequences as it is a strategy aimed at responding to an incident after it has occurred, and hence, it can only drive down likelihood. Ergo, Australia's deterrence-by-punishment strategy is aimed at reducing the likelihood of China launching disruptive cyber attacks.

Significantly, the loop in Figure 6.1 illustrates how Australia might maintain deterrence capabilities—with a focus on offensive capabilities and taking into account the issue of escalation—in response to malicious cyber incidents conducted by China. It is influenced by a more dynamic concept of deterrence, which considers operational frameworks for integrated deterrence and that informs the need for Australia to have a multitude of potential responses ready across various thresholds. It should also be emphasised that the model is an attempt to provide a normative and publicly debated value of cyber interactions.

This deterrence model is based on the three critical pillars that should feed into any strategy that Australia employs: credibility, technical capacity and communicative ability. In addition, this illustrative loop is in response to a confirmed incident (potentially in this case from China) but is not the entirety of the strategy. Hence, integrating and stress testing other relevant and complementary components such as those as captured by Libicki's (2009) framework can also be seen as crucial to understanding if this loop could be deployable in the first place—a loop that will need to conceivably incorporate a diversity of actors and threats. Nonetheless, for example, other questions to consider beyond 'Do we know who did it?' might include 'Can we hold their assets at risk; can we do so repeatedly; if retaliation does not deter, can it at least disarm; does retaliation send the right message to our own side; do we have a threshold for response; and what if the attacker has little worth hitting?'

A final consideration is that the loop is reactive and not proactive. Despite the significant increase in labour power for ASD through program such as REDSPICE, a proactive loop would require that teams constantly be assigned to monitor nations such as China, which is an insurmountable resource demand for Australia to meet. There is simply too much activity in the cyber domain from too many potential adversaries for Australia to commit a multitude of teams to each adversary and constantly create and confirm potential punishment strategies. Resources are better utilised in a reactive manner by instead utilising the loop in Figure 6.1 to craft potential responses at speed.

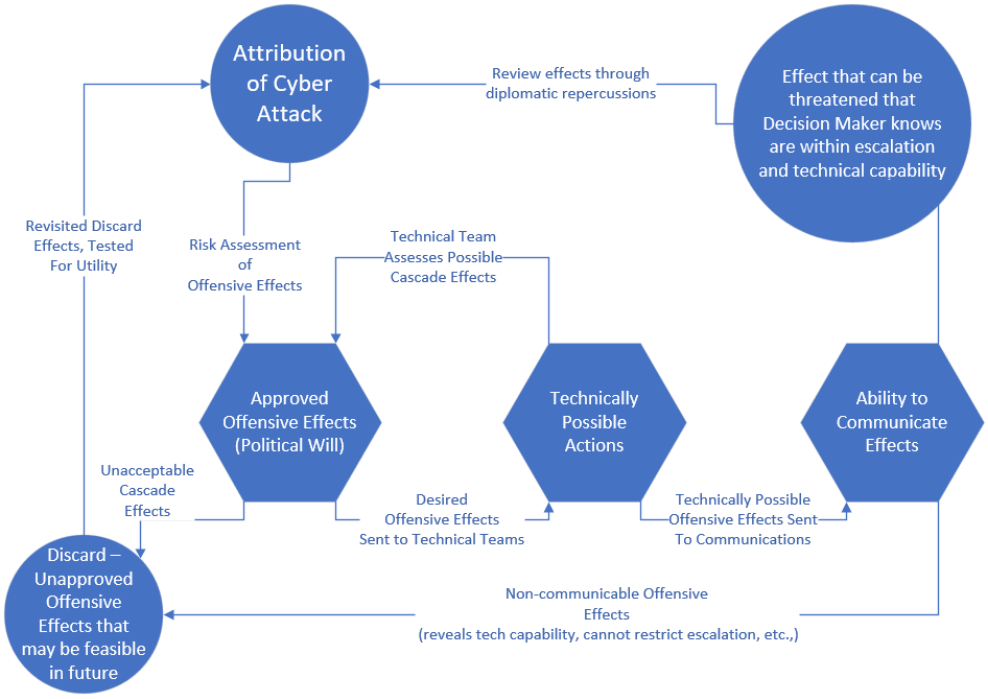

Figure 6.1: Deterrence Model

The process based on Figure 6.1 is explained in the next sections.

6.2.1 Attribution of Cyber Attacks

Purpose: To find 'Who did it?'—the process of identifying and tracking the perpetrator of a cyber attack.

To address the seriousness of the incident and the baseline of attribution. Generate a wide range of flexible ideas and ad hoc strategies for cyber operations, both offensive and defensive, and align these strategies with the operational and normative environment of cyber operations.

Example Activity: Target-specific attribution by using technical information, intelligence information and geo-strategic context is central. This stage may also involve undertaking collective attributions and related inputs with allied and like-minded partners.

6.2.2 Risk Assessment of Offensive Effects

Purpose: To evaluate the potential risks and effects of proposed offensive cyber operations, including unintended consequences and collateral damage.

Example Activity: Red teaming as a cybersecurity exercise. Conduct cost–benefit calculations and holistic analyses to identify and assess the implications of a proposed cyber strike on a Chinese city's power grid, which includes assessing the potential for escalation, civilian harm and international law implications.

6.2.3 Approved Offensive Effects (Political Will/Credibility)

Purpose: To perform a comprehensive risk assessment (that will include wider geopolitical considerations) to decide whether to proceed with a timely, credible offensive response combined with the political willingness to accept the risks and consequences as part of an instrument of national policy.

Example Activity: High-level government officials decide to authorise a cyber operation against China's military command and control systems after weighing the potential benefits and risks. The credibility of deterrence may also be undermined if the response is ambiguous.

6.2.4 Desired Offensive Effects Sent to Technical Teams

Purpose: To communicate the approved offensive plans to the technical teams who will execute them. As assessed in Chapter 2, these teams can be from ASD, AFP or the Department of Defence.

Example Activity: The strategic command sends detailed operation plans to the cyber unit to prepare malware that will disrupt enemy communications, living-off-the-land operations, etc. Black (2023) asserted that the new era of offensive operations prioritises exploiting vulnerabilities in an entity's existing software and is less reliant on malware. Regardless, this does not dismiss the utility of such operations, and they still have significant relevance.

6.2.5 Technically Possible Actions

Purpose: To develop and prepare cyber tools and methods that are technically feasible in order to achieve the desired offensive effects.

Example Activity: Cybersecurity professionals and programmers design and test a specific exploit against China's software vulnerability in a sandbox environment. Espionage operations may be conducted in this scenario to mimic the potential targeted environments, which decision-makers would need to be aware of and understand that this may also cause escalation.

6.2.6 Technically Possible Offensive Effects Sent to Communications

Purpose: To inform relevant domestic and international parties about the cyber operation, balancing transparency with the need for operational security.

Example Activity: A classified briefing to international partners about a covert cyber operation that has been successfully executed, without revealing sensitive details.

6.2.7 Effect That Can Be Threatened That Decision-makers Know Are Within Escalation and Technical Capability:

Purpose: To ensure that any threats or implied actions in the cyber domain are credible and within the nation's capability to execute without undesired escalation.

Example Activity: A government spokesperson makes a public statement alluding to the country's capability to respond to cyber aggression, as a deterrent.

6.2.8 Ability to Communicate Effects

Purpose: To reveal information about intent, resolve and capabilities. To deter and to shape the strategic decision-making process of Chinese officials, coercing them to act—or not act—in a manner desired by Australian strategists.

Example Activity: Messaging is crafted—and sent publicly or *sub rosa* through diplomatic channels—that should China conduct certain malicious activities, it can expect responses in kind that Australia considers proportionate, and that there are a multitude of responses available to Australia, including offensive operations that might 'manipulate, deny, disrupt, degrade or destroy targeted computers, information systems or networks'(Uren et al., 2018).

Decision is made about the communication channel to be used, that is, public or covert, to identify the perpetrator and the extent of evidence to be released.

Assessment of whether past deterrence messages, either public or *sub rosa,* about thresholds have been credible and have been received and clearly understood by China. Address whether an attack has crossed a key threshold, and deliberate whether any punishment action can be supported and legitimated by previous communications regarding resolve and the signalling of intent. In other words, have adversaries been made aware of the consequences of conducting a cyber attack?

6.2.9 Unacceptable Cascade Effects

Purpose: To identify and halt any cyber operations that could lead to uncontrollable or undesirable secondary effects and disadvantageous proliferation pressures.

Example Activity: Cancel a planned cyber attack on financial systems owing to the risk of a cascading effect on the Chinese economy that results in possible kinetic warfare repercussions.

6.2.10 Review Discarded Effects and Test for Utility:

Purpose: To reassess and possibly discard certain cyber strategies or tools based on their effectiveness or changes in utility.

Example Activity: Decommission a cyber weapon that is no longer effective because vulnerabilities in the target systems have been patched.

6.2.11 Strategic Review (Process End, Continuous Improvement Feedback to Brainstorm)

Purpose: To review and discard periodically outdated or compromised cyber tools and strategies to maintain operational effectiveness.

Example Activity: An audit of cyber tools in the national arsenal, removing those that have been exposed or are no longer operationally viable.

Based on the thesis lines of inquiry, this example model loop could indicate how Australia can maintain the application of deterrence policy, ready to deploy at speed to cyber incidents as part of a viable deterrence-by-punishment strategy. However, this loop is in response to a confirmed incident—in this case, from China—but is not the entirety of the strategy. Stress testing Libicki's (2009) framework is crucial to understanding if this loop could be deployable in the first place.

6.3 Research Findings from SWOT Analysis

As stated in Chapter 1, a final SWOT analysis will be utilised to determine the effectiveness of deterrence in the cyber domain, and also that of Libicki's (2009) framework, with a focus on punishment. This can inform Australian decision-makers about not only how to apply deterrence but also to do so in a way that controls escalation. There is no evidence that Australia

officially wants or desires a cyber incident to escalate beyond the cyber domain, but it does want to dissuade China from engaging in malicious cyber attacks.

6.3.1 Do We Know Who Did It?

6.3.1.1 Strengths

Australia has demonstrated on numerous occasions (described in Chapters 2 and 4) the political will and technical capacity to conduct attribution and publicly disclose the attribution naming another state, including China. This is a key foundation for effective deterrence. It has done this either alone or with partner states, and such partnerships can be seen as value adding and as a strength for both Australian capability and credibility (Holland & Chiacu, 2021). Australia not only has the capacity to conduct attribution but has done so repeatedly.

6.3.1.2 Weaknesses

As outlined in Chapter 4, a primary difficulty facing attribution often remains time and time lags, affecting concepts such as temporal continuity and contingency (Staddon & Cerutti, 2003). The inability to conduct quick and correct attribution can and will significantly hamper the legitimacy of retributive actions. It has not always been clear, or not always been sufficiently demonstrated by Australia, that attribution can produce actionable and reliable evidence in highly short time frames. The secrecy around such ASD operations has meant that such details are often not publicly revealed. Timeframes are arguably Australia's most significant weakness in attribution, especially if the punishment exacted in response is to be seen as legitimate and proportionate.

6.3.1.3 Opportunities

The political opportunity lies in the willingness and capacity of Australia to continue to publicly attribute cyber events or incidents involving China. The more Australia publicly attributes based on evidence, the more likely China will be held accountable for its actions—which may also transform deterrence ideas reliant solely on a defensive posture to those reliant on a more offensive posture as described above. In this sense, the emphasis on burden of proof would be less on convincing China of the attribution identification, but instead more on the perceptions of the Australian public and international allies about the merits of retaliation (Egloff, 2020a). Repeated cases of attribution will also build relevant skill sets in Australian

capital and labour, and hopefully enhance speed and accuracy. Further, a greater body of pre-existing public knowledge can add to the speed of attribution, not only because Australia will become more confident with attribution, but also because the international community will become more accustomed to hearing it.

6.3.1.4 Threats

Getting attribution wrong and launching a significant cyber attack against the incorrect target could have disastrous and counterproductive ramifications. Depending on the severity of the attack, a worst-case scenario could be that it triggers a kinetic conflict in response in which case, cyber deterrence has failed. Having such a significant point of failure makes attribution greatly important to deterrence by punishment. Another threat relating to attribution will be a loss of capability, or the inability to conduct attribution at the scale and speed required for an effective deterrence-by-punishment strategy to work.

6.3.2 Can We Hold Their Assets at Risk?

6.3.2.1 Strengths

It had been implied by the mission given to ASD (by former Prime Minister Turnbull) that Australia has some capacity to hold adversary entities' assets at risk, because it also implies offensive CNE, which is then the targeting of adversary networks and identifying vulnerable assets (T McKenzie, 2017). However, if there is insufficient data to confirm said identification, then arguably it would be unwise for Australia to publicly threaten an asset directly as it would alert China that Australia had conducted said CNE. It could be used as a tactic to send China on a 'wild goose chase' into its own systems, forcing them to harden networks and commit resources. However, doing this repeatedly would not only undermine Australian assertions of capability but also simply drive an improvement in Chinese cybersecurity of their assets. In short, it is better for Australia to remain opaque about the assets that it can hold at risk from a capability and retaliation perspective (of course, limited to cyberspace).

6.3.2.2 Weaknesses

A distinct and fundamental weakness that is built into the unique cyber-deterrence realm is that open specificity in threats to assets will lead to the loss of capability to threaten that asset, because the adversary will now know there is a deliberate target and a likely vulnerability that

they need to patch or address through actions such as password change or removal of default settings. Lacking the ability to credibly threaten a specific asset in a timely manner is a drawback for cyber deterrence as a whole.

6.3.2.3 Opportunities

If holding specific national assets as a threat is functionally impossible, analysing cost–benefit effects might be the next best option. As was discussed throughout the thesis, decision-makers are ill-advised to desire specific assets threatened or actioned anyway. Instead, they should ask IT teams to produce an action to affect desired political and/or psychological conditions to change behaviour (Seligman, 2022). This can be translated into the communication aspect of deterrence. For example, do not threaten a specific power grid, but threaten the functionality of industry. The related challenge of this opportunity is creating credible effects. In other words, make the effect too broad in scale and it would be simply unbelievable, and even if Australia could achieve it, the action might cross an unacceptable threshold. Before assets can be threatened, these effects would also need to be discussed with offensive agencies such as ASD determine the internal credibility of the threat— it would be a poor choice for Australia's executive to threaten effects beyond what is possible in reality or unworkable by the ASD. Moreover, there is no guarantee the threat will even work. As asserted in Chapter 3, China has a greater risk appetite than Australia. Hence, in short, it would be incalculably damaging for the credibility of Australian deterrence-by-punishment methods for the country to be openly exposed as either unwilling or incapable of acting on threats.

It is worth noting that, in 2023, Australian ports suffered a halt to operations because the largest ports operator, Dubai Ports World, an entity based in the United Arab Emirates, was hit by a cyber attack (Kruger, Swan, & Wright, 2023). The attack was so significant it 'constituted a supply shock, and a prolonged closure could push up prices of goods, which in turn would force the Reserve Bank to consider a further interest rate rise' (Kruger et al., 2023). At the time of writing, it is unclear who perpetrated the attack. However, it is indicative of the sort of effects and attack pathways available to states if they are willing to execute them, and the situation is serious enough that the AFP have been deployed to assist in mitigating the incident (Schultz & Peppiatt, 2023). Hence, rather than threaten an asset (e.g. the ports or their systems), a policy pathway or opportunity is to threaten functionality. The vulnerability in the port company may have already been found, and if China's critical assets or infrastructure are directly threatened in reprisal, it would do everything in its power to harden its own vulnerabilities. However, if

the supply chains that rely on these critical infrastructure operations or assets are instead held at threat, this threat could be issued repeatedly because of the multitude of points of failure, and these threats can also be seen as legitimate and proportionate because it is something that Australia has suffered itself.

6.3.2.4 Threats

Wild accusations and threats to non-existent assets are a significant threat to a legitimate posture from Australia since threats must be credible and, therefore, carefully considered. Thus, it is in Australia's national interests to avoid conveying threats that are hyperbole, inaccurate and immature. Australian threats should build from hard-headed risk assessments and valid political opportunities that can be accurately presented in public. China is a serious cyberthreat, but it should not be an exaggerated threat and nor should threat intelligence be politically misused for crude 'China-bashing' and fanning xenophobic sentiments.

6.4 Can We Do So Repeatedly?

6.4.1.1 Strengths

Functionally, changing threats to attack assets to threats to ensure effects makes the repeated threat pathway possible. The earlier iteration of threatening assets faced difficulties that are typically associated with the cyber domain, but threatening effects opens up too many possibilities for the defender to comprehensively ameliorate (Seligman, 2022). This is a significant strength for Australia.

6.4.1.2 Weaknesses

Escalation is a massive concern, particularly if the change is made from threatening assets to threatening effects. The issue could become a lack of surgical precision in responses, which may affect assets that the Chinese hold in far higher regard than Australian decision-makers at first understand. The communication of effects could also be interpreted by Chinese decision-makers as more inflammatory, as the effects could be something that occur throughout China whereas the Australian strategist only meant to threaten a specific asset and/or system. The potential 'cascade effects' of threatening to ensure just effects and not to attack specific assets also present a weakness in the strategy, as it may spin far beyond the decision-makers' intentions (Sharma, 2016, pp. 65–66).

6.4.1.3 Opportunities

Repeated capability amplifies threats. The ability to directly affect Chinese decision-makers so comprehensively because Australia could repeatedly inflict pain upon them at a strategic level is a threat that would affect the strategic and political decision-making of China. It is also useful as a thought exercise between strategic decision-makers and the operational and technical levels of Australian cyberwar that they can create numerous strategies for inflicting retribution across various networks, chasing an effect that does not cascade and cause unintended blowback.

6.4.1.4 Threats

As stated, escalation is a significant issue relevant to repeated threatening or acting upon effects. As discussed in the literature review, cascade effects are a likely outcome of offensive cyber operations, which can have ramifications that the attacker was unprepared for.

6.4.2 If Retaliation Does Not Deter, Can It At Least Disarm?

6.4.2.1 Strengths

The first objective in traditional war is to disarm the opponent (von Clausewitz, 1989). By adhering to this line of reasoning, Australia could use its cyber arsenal to engage with the idea of disarmament and seek to deploy it in abstract terms. However, it is difficult to envision what disarmament could possibly entail in the cyber realm and how it would be enforced.

6.4.2.2 Weaknesses

Libicki (2009) asserted that it is practically impossible to disarm an attacker because 'the perquisites for a cyber attack are few: talented hackers, intelligence on the target, exploits to match the vulnerabilities found through such intelligence, a personal computer … and any network connection' (pp. 59–61). Australia has few if any options for completely and unequivocally preventing the Chinese from satisfying the material and operational conditions for launching cyber attacks including via proxies. As described in Chapter 3, these cyber proxies can be hired for a particular operation or for organised groups of hackers, such as 4/PLA.

6.4.2.3 Opportunities

If disarmament is fundamentally impossible, then denial is the best option for Australia's defence. However, the silver lining, as Libicki (2009) put it, is 'if it is not possible to disarm the cyberattacker, there is little point to rushing into retaliation' (p. 62). The goal is to convince China not to try again. Decision-makers need to avoid feeling overwhelmed by the supposed light-speed of the cyber domain and remember that decisions still happen at the speed of a human brain, with human considerations.

6.4.2.4 Threats

Immaturity in public responses and short-sighted opportunistic desires directed at Australian cyber teams by Australian policymakers are threats. Decision-makers that task entities such as the ASD need to have a solid grounding in the limitations and implications of cyber operations and ensure that any political request for effects are actionable in reality. There are many connection points between Australia and China that also facilitate mutual advantages. Shutting them down is unlikely to be the answer to 'disarming' the Chinese, for it would simply crush the ability to initiate trade and other positive aspects of the China–Australia relationship.

6.4.3 Will Third Parties Join the Fight?

6.4.3.1 Strengths

Yes, and this is already evident. Third parties such as the US have already joined the fight, and they have joined on the side of Australia publicly. What started as a question down the line in the Libicki (2009) framework has evolved into one of the more far-reaching questions in 2023 and beyond. Australia regularly makes public attributions of Chinese cyber operations alongside Five Eyes partners which also signals the growing importance of intelligence agencies such as the ASD in the offensive aspect of cyber operations.

6.4.3.2 Weaknesses

Employing third parties in attribution may guarantee respectability but may also heighten anxiety in the target adversary state and therefore potentially enhance the likelihood of escalation. The likelihood is that China might feel more threatened and 'contained' when it is not only Australia but also the Five Eyes making public attribution and retaliation. In this situation, China must contend with multiple states in its own risk assessments and, in particular,

with the US, which is China's direct strategic competitor in the region. This could add to the intensifying rivalry between the US and China, and a US–China war would profoundly affect Australia.

6.4.3.3 Opportunities

The opportunity facing Australia is the capacity to enlist some of the most skilled, potent cyber actors on its side. The Five Eyes allies have not been completely transparent about the extent of intelligence sharing between them, but it is public knowledge that it occurs. Even if there is only the sharing of known vulnerabilities or exploits, it is a tremendous increase in Australia's capacity to launch offensive cyber operations against China. The continual showing of a united front also hardens Australian networks at the strategic level, as it reinforces to China that Australia will enlist its allies and that its allies will involve themselves. Existing treaties such as ANZUS and new treaties such as AUKUS and the Quad might also create strategic hedging that not only enhances Australian capability but also likely prevents escalation, because Chinese decision-makers must be aware that escalating against Australia greatly increases the likelihood of third parties joining the fight.

6.4.3.4 Threats

Escalation out of the cyber domain would be a primary concern in how Australia responds. Currently, when third parties have joined, it has only been in attribution (at least that is what is publicly known). However, if Australia and Five Eyes countries, ANZUS/AUKUS or the Quad were to launch joint offensive operations as retribution, then the strategic calculus of China would shift dramatically. Now multiple powerful states are threatening China, some of which are direct strategic competitors. As a starting point, Australia must exercise caution and diligence in enlisting the support of these allies and treaty partners in efforts to launch retributive actions.

6.4.4 Does Retaliation Send the Right Message to Our Own Side?

6.4.4.1 Strengths

Perhaps the best outcome for retaliation would be the type of collaboration required between Australia and its allies and the potential improvement in capabilities and skills that it could procure.

It would also benefit Australia if there could be an established 'best practice' among Five Eyes partners for retributive action via projects such as REDSPICE. Importantly, it would be especially useful at establishing among allies understanding about the actions or limits that are acceptable and not acceptable, even developing further into defining normative red lines that Australia and allies/treaty partners at least consistently agree upon. Consequently, despite the notion of collaboration, it may be that Australia and Australia alone carries out the function, but the country can also involve relevant third parties to improve accountability, oversight, potential development/improvements and the understanding that Australia's actions are not inherently seen as escalatory, at least by allied and treaty partners.

6.4.4.2 Weaknesses

Australia's allies (particularly the Five Eyes) have been publicly vocal about maintaining 'normal' behaviour in cyberspace and decrying offensive actions in the cyber domain, particularly those that provide commercial benefit to Chinese private entities by damaging non-Chinese private entities through degradation, destruction or theft of data. Because of this approach, retributive actions may be seen as at odds with Australia's stated position on cyberspace through documents such as the 2017 DWP from DFAT. Since it has committed to a stable and secure cyberspace, Australia would need to exercise caution and execute extremely carefully before engaging in retributive punishment action. Another weakness is time and time lags. Collaborating with a range of entities in various ways extends the time for response at Australia's disposal, unless the decision has been made, and collaboration mostly involves notifying third parties of events that have or will occur.

6.4.4.3 Opportunities

The aforementioned collaboration is an opportunity in a retributive action that has to some extent the involvement of Australian allies. Being able to draw on the expertise of allies and treaty partners is a tremendous strength in Australia's favour that Australian decision-makers should exploit. In short, functionally, it would demonstrate to the Chinese that Australian capabilities are Five Eyes capabilities.

6.4.4.4 Threats

Speed, complexity and time are threats. Engaging with multiple stakeholders, even if they are on Australia's side, adds complexity to the operation on which it seeks to embark. This adds

time, further constraining the temporal continuity and contingency in the Chinese strategic decision-maker's mind. Engaging these third parties on an ad hoc basis will be especially complex and time-consuming. It would need to be addressed early for Australia to have the means of communicating intent with groups such as the Quad or ANZUS and have the ability to quickly execute an agreed-upon pathway that can be reasonably executed. This adds incredibly complexity to the operations from a political and strategic standpoint.

6.4.5 Do We Have a Threshold for Response?

6.4.5.1 Strengths

The strength of thresholds would be to signal to friend and foe alike regarding activities Australia considers 'unacceptable' in the cyber domain that would compel it to act in a potentially punitive manner. Hopefully, it would help to explain why retributive actions were undertaken, both to the aggressor state and to Australia's own allies, addressing some of the concerns over proportionality and retaliation and sending the right message to Australia's own side.

6.4.5.2 Weaknesses

The nature of the cyber domain means that offensive operations can be launched with relative ease and also typically do not have such an impact that they would cause kinetic warfare to occur. Such warfare methods are not impossible, just improbable. The relevance is that stipulating clear thresholds that are unacceptable if crossed may instead just compel the Chinese to test these thresholds and determine whether Australia really means it. Although 'a missile down your smokestack' is a compelling quotation, if Australia levelled such gravitas on the protection of its electrical grid, what would stop the Chinese from checking whether Australia is serious and trying it out? Australia's worst-case scenario is escalation that causes a strategic conflict to leave the cyber domain and escalate to kinetic; thus, thresholds that threaten certain responses can be dangerous for Australia instead.

6.4.5.3 Opportunities

Thresholds present a usable thought exercise for Australia to clearly understand what it is willing to accept, and what it is not. This is important and must be done. Perhaps what is not necessary is to make public these thresholds—Australia could simply hold *sub rosa*

communications with allies, which may evolve into a shared security arrangement such as through ANZUS. It could also be an expansion of AUKUS, where shared security arrangements springboard from thresholds that Australia and her allies have already agreed upon in private first. Of course, whether and to what extent Australia might be engaged with *sub rosa* communications with China is currently unknown and classified.

6.4.5.4 Threats

Public thresholds could conceivability create an increase in activity as malicious actors, not just China, could see these as a challenge to prove whether Australia means it and is genuine when it creates these thresholds.

6.4.6 Can We Avoid Escalation?

6.4.6.1 Strengths

With Australia's steadily developing capabilities and the capabilities of its allies, a strength on offer to avoid escalation is the implied capacity to launch extremely precise operations. Identifying the desired effect and then clearly identifying the assets that should be threatened to achieve this effect can help give clarity about the operation and better inform the decision-maker whether it would be a suitable course of action.

6.4.6.2 Weaknesses

Cascade effects are a significant risk in the cyber domain (Sharma, 2016, pp. 65–66). Some networks are poorly designed and carry multiple points of failure (Andriole, 2021). In attempting to avoid hitting such a point of failure accidentally, further demands are imposed on the attacking team to be more precise, which means the attacker needs more time to determine the network layout and ensure precision. More time means the capacity for a deterrent effort to be directly correlated with a certain task is less likely. It poses an immense challenge to have legitimate offensive actions at Australia's disposal without conducting pre-positioning on Chinese networks, which in its own manner could be escalatory. Avoiding escalation is then a potential critical weakness in cyber deterrence.

6.4.6.3 Opportunities

Investigating methods that can unleash useful and powerful effects with precision is the most significant opportunity for Australia but is also extraordinarily difficult, to the point where if it were attainable, it is reasonable to assume that Australia would have attained it already. Barring technological developments that allow Australian offensive teams to quickly unravel security protocols or exploit vulnerabilities with extreme speed, pre-positioning is Australia's main response as a lone entity. Another opportunity could be calling upon allies, sourcing vulnerabilities that they may have found and exploiting them via an agency such as the ASD once the intelligence has been shared. A small example may be that the US NSA had uncovered a vulnerability in the Microsoft Operating System but had kept it quiet in order to exploit it, to the point that the US did not notify even allied nations and it created a series of bespoke cyber weapons to use that vulnerability. Perhaps, in future, Australia could request allied states to share intelligence whereby Australia receives knowledge of the vulnerability and copies of the cyber weapons and is able to tailor them to its needs and deploy them.

6.4.6.4 Threats

As has been stated earlier in the chapter, Australia's worst-case scenario is that the conflict in the cyber domain escalates to such an extent that one of the sides is compelled to deploy kinetic weapons. Australian decision-makers would need to carefully consider the risk appetite for escalation and investigate whether this appetite restricts any strategic contest to the cyber domain. Strategic-level attacks can occur in the cyber domain but do not have the same lasting effects as in kinetic warfare. For instance, even if an entire electric grid is degraded by a cyber attack, it is a matter of hours, not months or years, to return the grid to some form of operations (as demonstrated in Kyiv in 2015).

6.4.7 What If the Attacker Has Little Worth Hitting?

6.4.7.1 Strengths

Positively, China has an immense amount of assets worth hitting. The country is highly digitised with a large footprint; much of its critical infrastructure is, or in the process of being, digitised; and it has numerous government programs aimed at developing what is simply called 'digital China' (Weiduo, 2023).

6.4.7.2 Weaknesses

Clarity of choices and cascade effects are weaknesses. China's immense digitisation means an interoperable society, which can greatly enhance the potential damage of cyber weapons. Australian decision-makers must be aware that rather than this factor being a net good, it increases the risk that cyber weapons will spiral beyond the control and intention of Australian attackers, potentially triggering an escalation crisis.

6.4.7.3 Opportunities

The plurality of choices is an opportunity. Since China has such an extensive network footprint, offensive Australian operations, importantly the espionage aspect, can hopefully go undetected when seeking useful targets to trigger the desired effects.

6.4.7.4 Threats

The scale of digitisation occurring in China results in increasing the potential for cascading effects, which may lead to crisis escalation. It would take careful, controlled espionage operations to truly unpack the interconnected nature of Chinese networks and even then, it may not satisfy the risk needs of decision-makers. As regards strategic cyberwarfare-level attacks, Australia would need to exercise extreme caution before deploying offensive cyber weapons.

6.5 Suggestions for Future Research

Given the discussion in this chapter, it will be valuable to conduct further research on unintended effects (or game theory) as well as the role of the principle of proportionality in the more ambiguous 'grey zone'. Australia will require significantly more insight into potential cascade effects not only in the cyber domain but also with diplomatic or even kinetic warfare ramifications. It has been asserted throughout the thesis from Chapter 1 to Chapter 4 that cyber operations can have these cascading effects, but much of the literature does not truly delve into specific and potential cascade scenarios. It is especially necessary as governments change, and the risk appetite potentially evolves with that change—new decision-makers may be timid or aggressive. Thus, Australia will require a competent understanding of the extent of consequences in such scenarios.

In this respect, the impact of AI on offensive systems and especially as a responding system will need thorough investigation. The world is sleepwalking towards potential calamity with

AI and the automation of military response to very human-driven problems. Despite earlier assertions that cyber operations do not take place at the speed of light but at that of human thought, this small comfort could completely unravel in a future where retributive actions are algorithmically driven. Once cyberwarfare does in fact take place at light speed, human beings will be physiologically cut out of a conflict that they are incapable of comprehending. The proliferation of international talks on AI and potential norms building around the deployment of AI on military weapons systems may reflect this concern.

6.6 Concluding Statements (and Future of China–Australia Cyber Relations)

Deterrence is beset by a multitude of difficulties that are exceptionally unique to the cyber domain. Nevertheless, after reviewing the case study of Australia and China, of the realities of attribution, defining cyber attacks and unpacking the desires of the states, a pathway to attaining a coherent, cogent, deployable deterrence-by-denial and deterrence-by-punishment strategy is visible.

Libicki's (2009) framework is useful, and it provides said pathway that Australia can go down to formalise a response process, even if only at a high level, and speed up response times at the political and strategic level in order to decrease temporal continuity issues presented by its deterrence strategy and the argument that if too much time passes, deterrence does not succeed. Competition in the cyber domain benefits Australia in that the state can potentially match China, or at least has a far closer power gradient in this domain than in the kinetic field. Tying deterrence measures to cyber means gives Australia a more realistic chance of achieving strategic outcomes. The added advantage is there is a clear threshold that Australia must avoid crossing, namely, that any strategic contest must remain in the cyber domain. Rather than a limitation, this gives Australia clear guidance on aims it should aspire to achieve in the cyber domain.

The future of the Australia–China cyber relationship is difficult to fully predict. China has clearly indicated a willingness to conduct offensive cyber operations without regard to diplomatic blowback, or at least considers that the benefits of these operations outweigh the risks, such as the hack on Australian Parliamentary parties in 2019. Perhaps China still has this mentality, and deterrence measures will be required to affect China's risk calculus.

References

Abdollah, T, 2019, 23 June, US launched retaliatory strike against Iranian military computers, as cyber war escalates, *The Sydney Morning Herald*, accessed 14/3/2022. Retrieved from https://www.smh.com.au/world/middle-east/us-launched-retaliatory-strike-against-iranian-military-computers-as-cyber-war-escalates-20190623-p520fb.html

Aidone, D, 2022, *Medibank has suffered a 'significant cyber security incident'. Here's what we know so far,* SBS News. Retrieved from Medibank cyber attack: What we know so far about the 'significant' incident | SBS News

Alazab, M, 2022, *A new cyber taskforce will supposedly 'hack the hackers' behind Medibank breach. It could put a target on Australia's back,* The Conversation. Retrieved from A new cyber taskforce will supposedly 'hack the hackers' behind the Medibank breach. It could put a target on Australia's back (theconversation.com)

Anand, V, 2006, *Chinese Concepts and Capabilities in Information Warfare,* Manohar Parrikar Institute for Defense Studies and Analysis. Retrieved from Chinese Concepts and Capabilities of Information Warfare | Manohar Parrikar Institute for Defence Studies and Analyses (idsa.in)

Andrews, K, 2021, *Press Conference: Attribution of malicious cyber activity to China's Ministry of State Security* [Press release]. Retrieved from https://minister.homeaffairs.gov.au/KarenAndrews/Pages/press-conference-attribution-of-malicious-cyber-activity-to-chinas-ministry-of-state-security.aspx

Andriole, S, 2021, Too many single points of failure threaten our digital infrastructure — & they're multiplying, *Forbes*. Retrieved from Too Many Single Points Of Failure Threaten Our Digital Infrastructures — & They're Multiplying (forbes.com)

Areddy, J & Mozur, P, 2014, Meet 3PLA, China's version of the NSA, *Wall Street Journal*, accessed 9/5/2023. Retrieved from https://blogs.wsj.com/chinarealtime/2014/07/08/meet-3pla-chinas-version-of-the-nsa/

Australian Security Intelligence Organisation, 2002, *Report to Parliament 2001-2002,* , Canberra, Commonwealth of Australia

Attorney-General's Department, 2008, *Cyber Storm II: National cyber security exercise final report*, Commonwealth of Australia, Canberra. Retrieved from https://apo.org.au/node/1607

Attorney-General's Department, 2009, *Cyber security strategy*, Commonwealth of Australia, Canberra.

Auckburally, N, 2020, *Prime Minister Scott Morrison unveils 2020 cyber security strategy*, Macquarie Government. Retrieved from Macquarie Government - PM unveils the 2020 Cyber Security Strategy

Computer Emergency Response Team, 2000, *Security Bulletin: CERT Summary CS-2000-04: CERT Summary*, accessed 16/8/2022. Retrieved from https://auscert.org.au/bulletins/ESB-2000.378

Austin, G, 2014, *Cyber policy in China*, Polity Press, England, Cambridge, UK.

Austin, G, 2016a, *Australia rearmed! Future needs for cyber-enabled warfare*, University of New South Wales, Canberra.

Austin, G, 2016b, *The Australian government needs to be more open about the cyber threat from China*, The Conversation, Retrieved from http://theconversation.com/the-australian-government-needs-to-be-more-open-about-the-cyber-threat-from-china-64549

Austin, G, 2016c, Avoiding groupthink on China, *The Diplomat*, accessed 26 October 2017. Retrieved from http://thediplomat.com/2016/10/avoiding-groupthink-on-china/

Austin, G, 2016d, Evaluating China's cyber power, *The Diplomat*, accessed 20 October 2017. Retrieved from http://thediplomat.com/2016/10/evaluating-chinas-cyber-power/

Austin, G, 2016e, 'Middle powers and cyber-enabled war: The imperative of collective security', in C. Samuel & M. Sharma (Eds.), *Securing cyberspace* (pp. 23–56), Pentagon Press, New Delhi.

Austin, G, 2018, How good are China's cyber defenses?, *The Diplomat*, accessed 24 December 2018. Retrieved from https://thediplomat.com/2018/07/how-good-are-chinas-cyber-defenses/

Austin, G, 2023, *Deterring China isn't all about submarines. Australia's 'cyber offence' might be its most potent weapon*, The Conversation. Retrieved from Deterring China isn't all about submarines. Australia's 'cyber offence' might be its most potent weapon (theconversation.com)

Australian Associated Press, 2020, 20 June, *China's denial of cyber attack 'laughable nonsense' says think-tank* [Press release], accessed 11/1/2022. Retrieved from https://www.9news.com.au/national/cyber-attack-australia-china-blamed-denies-hacking/43c4244c-8e3a-4275-b9be-ab106503e056

Australian Cyber Security Centre, 2016, *ACSC threat report*, Australian Signals Directorate, Canberra.

Australian Cyber Security Centre, 2017, *Strategies to mitigate cyber security incidents* [Media release], accessed 1/4/2022. Retrieved from https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents

Australian Cyber Security Centre, 2020, Glossary, accessed 18 March 2022. Retrieved from https://www.cyber.gov.au/acsc/view-all-content/glossary/c

Australian Cyber Security Centre, 2022a, *ACSC annual cyber threat report*, Australian Signals Directorate, Canberra. Retrieved from ASD's ACSC Annual Cyber Threat Report, July 2021 to June 2022 | Cyber.gov.au

Australian Cyber Security Centre, 2022b, *Information security manual*, accessed 14/4/2022. Retrieved from https://www.cyber.gov.au/acsc/view-all-content/ism

Australian Federal Police, 2004, *Annual report: 2003-2004*. Retrieved from https://www.righttoknow.org.au/request/4043/response/10684/attach/5/afp%20annual%20report%202003%202004.pdf

Australian Government Directory, 2021, *Computer Emergency Response Team Australia*, [Media release], accessed 1/4/2022. Retrieved from https://www.directory.gov.au/portfolios/defence/department-defence/computer-emergency-response-team-australia

Australian government slams Chinese hacking group over stealing company secrets, 2018, news.com.au, accessed 9/5/2023. Retrieved from https://www.news.com.au/technology/online/hacking/australian-government-slams-chinese-hacking-group-over-stealing-company-secrets/news-story/37f4a47cf309c4c5fcd5b01666a9813d

Australian National Audit Office, 2017, *Cyber resilience: ANAO Report No. 53*, Commonwealth of Australia, Canberra, accessed 11/4/2022. Retrieved from https://www.anao.gov.au/sites/default/files/ANAO_Report_2017-2018_53a.pdf

Australian Signals Directorate, n.d.-a, *What we do: REDSPICE*, Australian Government, Canberra. Retrieved from REDSPICE | Australian Signals Directorate (asd.gov.au)

Australian Signals Directorate, 2023, *People's Republic of China state-sponsored cyber actor living off the land to evade detection* [Joint Cybersecurity Advisory]. Retrieved from People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection | Cyber.gov.au

Australian Signals Directorate, 2013, *'Top 4' strategies to mitigate targeted cyber intrusions: Mandatory requirement explained*, Commonwealth of Australia, Canberra. Retrieved from https://apo.org.au/node/34993

Australian Signals Directorate, 2020, *Annual report 2019-2020*, Australian Government, accessed 4 April 2022. Retrieved from https://www.transparency.gov.au/annual-reports/australian-signals-directorate/reporting-year/2019-20-7

Australian Signals Directorate, 2022, *About* [Media release], accessed 14 April 2022. Retrieved from https://www.asd.gov.au/about

Bajkowski, J, 2023, *'Systems of National Significance' numbers double under critical infrastructure cyber crackdown*, TheMandarin. Retrieved from Cyber security systems of national significance numbers double (themandarin.com.au)

Baldino, D, 2023, *Eavesdroppers, code-breakers and digital snoops: A deep dive into one of the most secretive branches of Australian intelligence*, The Conversation. Retrieved from Eavesdroppers, code-breakers and digital snoops: a deep dive into one of the most secret branches of Australian intelligence (theconversation.com)

Baldor, L, 2011, *Cyber security added to US-Australia treaty*, NBC News. Retrieved from Cyber security added to US-Australia treaty (nbcnews.com)

Banks, W, 2021, Cyber attribution and state responsibility, *International Law Studies*, vol. 97. Issue 1. No. 43. Pp. 1038-1072. Retrieved from viewcontent.cgi (usnwc.edu)

Barbaschow, A, 2021, *ASD says cyber attack intervention will be 'rare' under critical infrastructure Bill*, ZDNet. Retrieved from https://www.zdnet.com/article/asd-says-cyber-attack-intervention-will-be-rare-under-critical-infrastructure-bill/

Bartos, C, 2016, *Cyber Weapons are not Created Equal*, U.S. Naval Institute, Proceedings 142/6/1: 30-33. http://hdl.handle.net/10945/49618

Bassi, J, 2023, *Collective consistency is the answer to Beijing's trade coercion*, The Strategist, Australian Strategic Policy Institute. Retrieved from Collective consistency is the answer to Beijing's trade coercion | The Strategist (aspistrategist.org.au)

Bateman, S, 2016, The Strategist, Australian Strategic Policy Institute, accessed 21 September 2016. Retrieved from http://www.aspistrategist.org.au/south-china-sea-arbitration-ruling-two-months/

Baughman, J, 2022, *'Unrestricted warfare' is not China's master plan*, China Aerospace Studies Institute, Air University. Retrieved from 2022-04-25 Unrestricted Warfare is not China's master plan.pdf (af.edu)

Beazley, K, 2003, Whither the San Francisco Alliance System?, *Australian Journal of International Affairs*, vol. 57, no. 2, pp. 325-338

Bebber, J, 2017, *Beijing's views on norms in cyberspace and cyber warfare strategy pt.2*, CIMSEC, accessed 31 July 2018. Retrieved from http://cimsec.org/beijings-views-norms-cyberspace-cyber-warfare-strategy-pt-2/33100

Bergman, R, & Mazetti, M, 2023, The battle for the world's most powerful cyberweapon, *The New York Times*. Retrieved from The Battle for the World's Most Powerful Cyberweapon - The New York Times (nytimes.com)

Berman, N, Maizland, L, & Chatzky, A, 2023, *Is China's Huawei a threat to U.S national security?*, Council on Foreign Relations. Retrieved from Is China's Huawei a Threat to U.S. National Security? | Council on Foreign Relations (cfr.org)

Besser, L, & Sturmer, J, 2016, 29 August, *Chinese hackers behind defence Austrade security breaches*, ABC News, accessed 13 August 2018. Retrieved from http://www.abc.net.au/news/2016-08-29/chinese-hackers-behind-defence-austrade-security-breaches/7790166

Bhattacharjee, Y, 2023, The daring ruse that exposed China's campaign to steal American secrets, *The New York Times*. Retrieved from The Daring Ruse That Exposed China's Campaign to Steal American Secrets - The New York Times (nytimes.com)

Bildt, C, 2017, *Why technology, not geography, is key to cybersecurity*, HuffPost, accessed 15/3/2022. Retrieved from https://www.huffpost.com/entry/technology-cybersecurity_b_8391152

Bing, C, 2017, *How China's cyber command is being built to supersede its U.S. military counterpart*, CyberScoop. Retrieved from How China's SSF is being built to supersede its U.S. military counterpart - CyberScoop

Biscoe, C, 2018, Sophisticated cyber attacks are biggest technology concern in 2018 [Web log post], IT Governance, accessed 15/3/2022. Retrieved from https://www.itgovernance.co.uk/blog/sophisticated-cyber-attacks-are-biggest-technology-concern-in-2018

Black, D, 2023, *Russia ushers in a new era of cyber-physical attack*, BindingHook. Retrieved from Russia ushers in a new era of cyber-physical attack - Binding hook

Blaxland, J, 2019, *A Geostrategic SWOT Analysis for Australia*, Australian National University, The Centre of Gravity Series. Retrieved from Centre of Gravity Series 49 - A Geostrategic SWOT Analysis for Australia (anu.edu.au)

Blinken, A, 2021, *Responding to the PRC's destabilizing and irresponsible behaviour in cyberspace* [Press statement], U.S. Department of State, Washington D.C., accessed 5/5/2022. Retrieved from https://www.state.gov/responding-to-the-prcs-destabilizing-and-irresponsible-behavior-in-cyberspace/

Borghard, E, & Lonergan, S, 2019, Cyber operations as imperfect tools of escalation, *Strategic Studies Quarterly – Perspectives*. Vol 13. Issue 3. Retrieved from Cyber Operations as Imperfect Tools of Escalation (af.edu)

Borys, S, 2019a, *Licence to hack: Using a keyboard to fight Islamic State*, ABC News. Retrieved from Licence to hack: using a keyboard to fight Islamic State - ABC News

Borys, S, 2019b, *Inside a massive cyber hack that risks compromising leaders across the globe*, ABCNews. Retrieved from Inside a massive cyber hack that risks compromising leaders across the globe - ABC News

Botsman, R, 2017, Big data meets Big Brother as China moves to rate its citizens, *Wired Magazine*, accessed 14 November 2017. Retrieved from http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

Brangwin, N, & Portillo-Castro, 2019, *Cybersecurity*, Parliament of Australia, accessed 26/3/2022. Retrieved from https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook46p/Cybersecurity

Brenner, S W, 2007, At light speed: Attribution and response to cybercrime/terrorism/warfare, *Criminal Law & Criminology*, vol. 97, no. 2, pp. 379–479.

Brodtman, G, 2019, *Australia's 2020 cybersecurity strategy: Defining the mission*, The Strategist, Australian Strategic Policy Institute, accessed 14/4/2022. Retrieved from https://www.aspistrategist.org.au/australias-2020-cybersecurity-strategy-defining-the-mission/

Brown, A, 2022, New laws to crack down on data hacking, *The Canberra Times*. Retrieved from New laws to crack down on data hacking | The Canberra Times | Canberra, ACT

Bucci, N, 2022, Claire O'Neil warns of new world of 'relentless' cyber-attacks after Medibank hack, *The Guardian*. Retrieved from Clare O'Neil warns of new world of 'relentless' cyber-attacks after Medibank hack | Cybercrime | The Guardian

Buchanan, B, 2017, *The legend of sophistication in cyber operations*, Cyber Security Project, Belfer Center, Cambridge, Massachusetts

Buchanan, B, & Rid, T, 2014, Attributing cyber attacks, *Journal of Strategic Studies*, vol. 4, no. 37. P 4-37, https://doi.org/10.1080/01402390.2014.977382

Bunker, R J, 2000, Unrestricted warfare: Review Essay I, *Small Wars & Insurgencies*, vol. 11, no. 1, pp. 114–121. https://doi.org/10.1080/09592310008423265

Burke, H, 2021, *Senator and academic warn of 'relentless' cyber attacks from China*, news.com.au, available at: https://www.news.com.au/national/politics/senator-and-academic-warn-of-relentless-cyber-attacks-from-china/news-story/32f511b3996f79370d7c8c4a6948d17e

Burke, E & Gunness, K & Cooper, C & Cozad, M, (2020), PLA Operational Concepts, 10.7249/RRA394-1.

Bushell-Embling, D, 2020, *ACSC details 'copy-paste compromise' attacks*, GovTechReview, accessed 22/02/2022. Retrieved from https://www.govtechreview.com.au/content/gov-security/news/acsc-details-copy-paste-compromise-attacks-656922750

Carvin, S, 2021, *The name, blame, shame game: Are cyber attributions useful?*, Centre for International Governance Innovation, accessed 5/5/2022. Retrieved from https://www.cigionline.org/articles/the-name-blame-shame-game-are-cyber-attributions-useful/

Cavelty, M D, & Wenger, A, 2020, Cyber security meets security politics: Complex technology, fragmented politics, and networked science, C*ontemporary Security Policy*, vol. 41, no. 1, 5–32, https://doi.org/10.1080/13523260.2019.1678855

Chabrow, E, 2009, *Why strategic cyberwarfare shouldn't be a military priority*, GovInfoSecurity. Retrieved from Why Strategic Cyber Warfare Shouldn't Be a Military Priority (govinfosecurity.com)

Chase, M S, & Moroney, J D P, 2020, *Regional responses to U.S.-China competition in the Indo-Pacific: Australia and New Zealand*, RAND Corporation, Santa Monica, CA. Retrieved from https://www.rand.org/pubs/research_reports/RR4412z1.html

Cheng, D, 2017, *Cyber dragon: Inside China's information warfare and cyber operations*, Praeger Security International, Santa Barbara, CA.

Cheng, D, 2000, 'Unrestricted warfare: Review Essay II', *Small Wars and Insurgencies*, vol. 11, no. 1, pp. 122-123

China Aerospace Studies Institute, 2021, *Science of Military Strategy (2013)*, In Their own words: Foreign military thought, Air University, Project Everest. Retrieved from Microsoft Word - 2021-01-04 Chinese Military Thoughts- In their own words Science of Military Strategy 2013.docx (af.edu)

China Aerospace Studies Institute, 2022, *Science of Military Strategy (2020)*, In their own words: Foreign military thought, Air University, Project Everest. Retrieved from 2022-01-26 2020 Science of Military Strategy.pdf (af.edu)

China hits back at 'fabricated' US hacking allegations, 2021, Al Jazeera. Retrieved from China hits back at 'fabricated' US hacking allegations | Science and Technology News | Al Jazeera

China rejects accusations of cyber attacks by Australia and its allies, 2021, ABC News. Retrieved from China rejects accusations of cyber attacks by Australia and allies - ABC News

Church, N, Brangwin, N, Dyer, S, & Watt, D, 2015, *Defending Australia: A history of Australia's Defence White Papers*, Analysis and Politics Observatory. Retrieved from http://apo.org.au/node/56886

Clapper, J R, 2017, 'Foreign cyber threats to the United States', John McCain (ed), Committee on Armed Services, One Hundred Fifteenth Congress, 5 January

Clark, R, 2021, *How Australia came to ban Huawei*, LightReading, accessed 9/5/2023. Retrieved from https://www.lightreading.com/asia/how-australia-came-to-ban-huawei/d/d-id/769688#:~:text=Australia's%20formal%20ban%20on%20Huawei,of%2014%20grievances%20against%20Australia.

Clarke, M, Hsu, J, & Peng, Z, 2023, Where are Australia-China relations headed?, *The Diplomat*. Retrieved from Where Are Australia-China Relations Headed? – The Diplomat

Clay, M, & Lee, R, 2022, *Unmasking the Devil in the Chinese Details: A Study Note on the Science of Military Strategy 2020*, China Aerospace Studies Institute, Air University, available at: https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2022-01-24%20SMS%202020%20in%20Perspective.pdf

Coble, S, 2022, *Australian government to invest $9.9bn in cyber*, infosecurity-magazine, accessed 19/5/2022. Retrieved from https://www.infosecurity-magazine.com/news/australian-government-to-invest/

Commonwealth of Australia, 2004, *Parliamentary debates*, Parliament of Australia, House of Representatives, Vol. 40, 3 August 2004, accessed 28 March 2022. Retrieved from https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=CHAMBER;id=ch

amber%2Fhansardr%2F2004-08-03%2F0180;query=Id%3A%22chamber%2Fhansardr%2F2004-08-03%2F0129%22

Coppel, N, & Chang, L, 2020, *Cybercrime, deterrence and evading attack*, The Strategist, Australian Strategic Policy Institute, accessed 27/4/2022. Retrieved from https://www.aspistrategist.org.au/cybercrime-deterrence-and-evading-attack/

Cordesman, A, 2019, *China's new 2019 defense white paper*, Centre for Strategic and International Studies. Retrieved from China's New 2019 Defense White Paper (csis.org)

Cordesman, A, Burke, A, & Molot, M, 2019, *China and the U.S.: Advanced modernization and preparation for war*, Center for Strategic and International Studies. Retrieved from http://www.jstor.com/stable/resrep22586.45

Council on Foreign Relations, n.d., *PLA Unit 61398*, Council on Foreign Relations. Retrieved from PLA Unit 61398 | CFR Interactives

Council on Foreign Relations, 2018, *Cyber operations tracker*, accessed 6 September 2019. Retrieved from https://www.cfr.org/cyber-operations/

Counter Adversary Operations, 2014, Hat-tribution to PLA Unit 61486 [Web log post], *CrowdStrike*. Retrieved from Hat-tribution to PLA Unit 61486 - crowdstrike.com

Cousin, G, 2005, Case study research, *Journal of Geography in Higher Education*, vol. 29, no. 3, pp. 421–427.

Coyle, S, 2021, *Australia's defence and national security: How defence is enabling Australia's cyber resilience*, The Cove, Department of Defence. Retrieved from Australia's Defence and National Security: How Defence is Enhancing Australia's Cyber Resilience | The Cove (army.gov.au)

Coyne, A, 2016, *Govt to spend $230m on cyber security strategy*, itNews, accessed 12/4/2022. Retrieved from https://www.itnews.com.au/news/govt-to-spend-230m-on-cyber-security-strategy-418409

Coyne, A, 2017, *Australia has created a cyber warfare unit*, itNews, accessed 4/4/2022. Retrieved from https://www.itnews.com.au/news/australia-has-created-a-cyber-warfare-unit-467115

Coyne, A, 2018, *MacGibbon to lead Australian Cyber Security Centre*, itNews, accessed 5/4/2022. Retrieved from https://www.itnews.com.au/news/macgibbon-to-lead-australian-cyber-security-centre-468628

Cozard, M R, 2016, *PLA joint training and implications for future expeditionary capabilities*, RAND Corporation, Santa Monica, CA.

Craigen, D, Diakun-Thibault, N, & Purse, R, 2014, Defining cybersecurity. *Technology Innovation Management Review*, vol. 4, issue 10, pp. 13–21. http://doi.org/10.22215/timreview/835

Croft, D, 2023a, *Australia is the 'weakest link' in AUKUS cyber security*, cyberdaily.au. Retrieved from Australia is the 'weakest link' in AUKUS cyber security - Cyber Daily

Croft, D, 2023b, *'It will come out' – the importance of mandatory reporting, with Rapid7's Raj Samani*, cyberdaily.au. Retrieved from 'It will come out' — the importance of mandatory reporting, with Rapid7's Raj Samani - Cyber Daily

CrowdStrike Global Intelligence Team, 2014, *CrowdStrike intelligence report: PutterPanda*, accessed 13/6/2022. Retrieved from https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

CrowdStrike, 2019, *Intelligence report: Huge fans of your work*. Retrieved from BLOG SERIES_Huge Fan of Your Work (passle-net.s3.amazonaws.com)

Crozier, R, 2018, *Australian Cyber Security Centre finally gets its own office*, itNews, accessed 5/4/2022. Retrieved from https://www.itnews.com.au/news/cyber-security-centre-opens-in-new-canberra-facility-500338

Crozier, R, 2023, *ASD takes cyber offensive to 'tens' of targets in the last year*, itnews. Retrieved from ASD takes cyber offensive to 'tens' of targets in the last year - Security - iTnews

Cybersecurity & Infrastructure Security Agency, 2023, *People's Republic of China state-sponsored cyber actor living off the land to evade detection* [Advisory]. Retrieved from People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection | CISA

Cyber war: Four corners, 2016 [Television program], Australian Broadcasting Corporation, Sydney.

Dahm, M, 2021, *China's Desert Storm education*, U.S. Naval Institute. Retrieved from China's Desert Storm Education | Proceedings - March 2021 Vol. 147/3/1,417 (usni.org)

Davies, A, Lewis, J, Herrera-Flanagan, J, & Mulvenon, J, 2012, *ANZUS 2.0: Cybersecurity and Australia-US relations*, Australian Strategic Policy Institute. Retrieved from SR46_cybersecurity_v2.pdf (amazonaws.com)

Davis, J H, & Sanger, D E, 2016, 15 December, Obama says US will retaliate for Russia's election meddling, *The New York Times*, accessed 16 December 2016. Retrieved from https://www.nytimes.com/2016/12/15/us/politics/russia-hack-election-trump-obama.html

Davis, P K, 2015, Deterrence, influence, cyber attack, and cyberwar, *New York University Journal of International Law and Politics*, vol. 47, no. 2, pp. 327–355. Retrieved from https://www.rand.org/pubs/external_publications/EP50950.html

Deeks, A, 2013, The geography of cyber conflict: Through a glass darkly, *International Law Studies*, vol. 89, accessed 27/4/2022. Retrieved from https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1043&context=ils

Defence Science and Technology Group, 2022, *STRATEGY: Information warfare*, accessed 5/4/2022. Retrieved from https://www.dst.defence.gov.au/strategy/star-shots/information-warfare

Defence Science and Technology Organisation, 2014, *Cyber 2020 Vision: DSTO cyber science and technology plan*, Canberra, Commonwealth of Australia. Retrieved from Cyber-2020-Vision.pdf (defence.gov.au)

Demers, J, & Evanina, W, 2020, *Rob, replicate and replace: China's global technology theft and how to counter it*, Paper presented at the RSAConference in San Francisco, California, United States. Retrieved from https://www.rsaconference.com/library/presentation/usa/2020/rob-replicate-and-replace-chinas-global-technology-theft-and-how-to-confront-it

Denning, D E, 2015, 1 April, Rethinking the cyber domain and deterrence, *Joint Force Quarterly*, no. 77, accessed 1/1/2022. Retrieved from https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-77/Article/581864/rethinking-the-cyber-domain-and-deterrence/

Department of Defence, 2000, *Defence 2000: Our future defence force* [White paper]. Retrieved from https://defence.gov.au/publications/wpaper2000.pdf

Department of Defence, 2016, *2016 Defence White Paper*, accessed 16 September 2016. Retrieved from http://www.defence.gov.au/whitepaper/Docs/2016-Defence-White-Paper.pdf

Department of Defence, 2017, *Information Warfare Division* [Media release], accessed 5/4/2022. Retrieved from https://defence.gov.au/jcg/iwd.asp

Department of Defence, 2020, *2020 force structure plan* [White paper]. Retrieved from https://www.defence.gov.au/about/publications/2020-force-structure-plan

Department of Defence, 2021, *Exercise Talisman Sabre 2021 officially ends* [Media release], accessed 26/3/2022. Retrieved from https://news.defence.gov.au/media/media-releases/exercise-talisman-sabre-2021-officially-ends

Department of Defence, 2023a, Cyberwarfare operations. Retrieved from Cyberwarfare operations | DST (defence.gov.au)

Department of Defence, 2023b, *Taking cyber warfare training to new heights* [Press release]. Retrieved from Taking cyber warfare training to new heights | Defence

Department of Foreign Affairs and Trade, 2010, *Australia-United States ministerial consultations 2010 joint communique* [Media release], accessed 23/8/2022. Retrieved from https://www.dfat.gov.au/geo/united-states-of-america/ausmin/Pages/ausmin-joint-communique-2010

Department of Foreign Affairs and Trade, 2011, *Australia-United States ministerial consultations (AUSMIN) 2011 joint communique* [Media release], accessed 23/8/2022. Retrieved from https://www.dfat.gov.au/geo/united-states-of-america/ausmin/Pages/ausmin-joint-communique-2011

Department of Foreign Affairs and Trade, 2012, *Australia-United States ministerial consultations 2012 joint communique* [Media release], accessed 23/8/2022. Retrieved from https://www.dfat.gov.au/geo/united-states-of-america/ausmin/Pages/ausmin-joint-communique-2012

Department of Foreign Affairs and Trade, 2017a, *Ambassador for Cyber Affairs and Digital Technology* [Press release], accessed 11/4/2022. Retrieved from https://www.dfat.gov.au/about-us/our-people/homs/ambassador-for-cyber-affairs

Department of Foreign Affairs and Trade, 2017b, *Australia's International Cyber Engagement Strategy*. Retrieved from https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf .

Department of Foreign Affairs and Trade, 2022, *Fifth India-Australia cyber policy dialogue*. Retrieved from Fifth India-Australia Cyber Policy Dialogue | Australia's International Cyber and Critical Tech Engagement (internationalcybertech.gov.au)

Department of Home Affairs, 2020, *Australia's cyber security strategy 2020*, Commonwealth of Australia, Canberra.

Department of Home Affairs, 2023, *Engagement on critical infrastructure reforms*. Retrieved from Engagement on critical infrastructure reforms (homeaffairs.gov.au)

Department of the Prime Minister and Cabinet, 2016, *Australia's cyber security strategy.* Retrieved from https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf

Depp, M, 2020, *The unsettled question of offense vs defense in cyberwarfare*, RealClear Defense. Retrieved from The Unsettled Question of Offense vs Defense in Cyberwarfare | RealClearDefense

Develle, Y, 2016, *The attribution game: The challenges and opportunities of cyber attribution in policy-making*, Medium, accessed 27/4/2022. Retrieved from https://medium.com/wonk-bridge/the-attribution-game-the-challenges-and-opportunities-of-cyber-attribution-in-policy-making-3f99cdacd586

Dillon, L, 2019, *First official Australian 'cyber crisis' highlights growing threat*, Defence Connect, accessed 1/1/2022. Retrieved from https://www.defenceconnect.com.au/intel-cyber/4991-first-official-australian-cyber-crisis-highlights-growing-threat

Dinstein, Y, 2012, The principle of distinction and cyber war in international armed conflicts, *Journal of Conflict and Security Law*, vol. 17. no. 2, 261–277. Retrieved from http://www.jstor.org/stable/26296230

Dorfman, Z, 2021, Tech giants are giving China a vital edge in espionage, *The Australian Financial Review*, accessed 13/4/2022. Retrieved from https://www.afr.com/technology/tech-giants-are-giving-china-a-vital-edge-in-espionage-20210107-p56sbr

Dortmans, P J, Thakur, N, & Ween, A, 2015, Conjectures for framing cyberwarfare, *Defense and Security Analysis*, vol. 31, no. 3, pp. 172-184. https://doi.org/10.1080/14751798.2015.1056935

Dreyfus, M, 2022, *Tougher penalties for serious data breaches* [Media release], Attorney-General's Department. Retrieved from Tougher penalties for serious data breaches | Our ministers – Attorney-General's portfolio (ag.gov.au)

Dunn, M, 2005, *A comparative analysis of cybersecurity initiatives worldwide*, Paper presented at the WSIS Thematic Meeting on Cybersecurity, International Telecommunication Union, Geneva.

Dunn, W.N. 2012, *Public Policy Analysis: An Integrated Approach (5th ed.),* Routledge. https://doi.org/10.4324/9781315663012

Dupont, A, 2015, *Full spectrum defence: Re-thinking the fundamentals of Australian defence strategy*, The Lowy Institute, accessed 16/8/2022. Retrieved from https://www.lowyinstitute.org/publications/full-spectrum-defence-re-thinking-fundamentals-australian-defence-strategy

Dutton, P & Hastie, A, 2022, *ASD unveils new facility in the face of tomorrow's threats* [Joint media release]. Retrieved from 8483358.pdf;fileType=application/pdf (aph.gov.au)

Dyment, J, 2018, 28 December, *The cyber attribution dilemma: 3 barriers to cyber deterrence*, SecurityIntelligence, accessed August 12, 2019, https://securityintelligence.com/the-cyber-attribution-dilemma-3-barriers-to-cyber-deterrence/.

Edwards, S, & Handler, S, 2021, *The 5x5-How retaliation shapes cyber conflict*, Atlantic Council. Retrieved from The 5×5—How retaliation shapes cyber conflict - Atlantic Council

Egloff, F J, 2020a, Contested public attributions of cyber incidents and the role of academia, *Contemporary Security Policy*, vol. 41, no. 1, 55–81. https://doi.org/10.1080/13523260.2019.1677324

Egloff, F J, 2020b, Public attribution of cyber intrusions, *Journal of Cybersecurity*, vol. 6, no. 1, tyaa012. https://doi.org/10.1093/cybsec/tyaa012

Eichensehr, K, 2020, *The law & politics of cyberattack attribution* [Public law research paper No. 19-36], UCLA Law Review, UCLA School of Law. Retrieved from The Law & Politics of Cyberattack Attribution by Kristen Eichensehr :: SSRN

Erickson, Andrew S. (2007) *The Science of Military Strategy*, Naval War College Review: Vol. 60: No. 3, Article 11. Available at: https://digital-commons.usnwc.edu/nwc-review/vol60/iss3/11

Evans, L, 2022, *Home Affairs Minister Clare O'Neil urges a 'good thorough' look into Optus' management after major cyberattack*, Sky News. Retrieved from Home Affairs Minister Clare O'Neil urges a 'good thorough' look into Optus' management after major cyberattack | Sky News Australia

Evans, J, 2021, *Home Affairs Minister vows to continue to hold China accountable for cyber attacks*, ABC News, accessed 22/02/2022. Retrieved from https://www.abc.net.au/news/2021-07-20/china-hack-microsoft-international-blame/100306254

Fallon, S, 2022, *Cybersecurity package*, Parliament of Australia, Canberra. Retrieved from Cybersecurity package – Parliament of Australia (aph.gov.au)

Farley, R, 2014, What scares China's military: The 1991 Gulf War, *The National Interest*, accessed 29 December 2018. Retrieved from https://nationalinterest.org/feature/what-scares-chinas-military-the-1991-gulf-war-11724

Farley, R, 2019, Making sense of 'cyber-restraint': The Australia-China case, *The Diplomat*, accessed September 9, 2023. Retrieved from Making Sense of 'Cyber-Restraint': The Australia-China Case – The Diplomat

Faulkner, J, 2010, *Cyber Security Operations Centre officially opened* [Media release], accessed 28/3/2022. Retrieved from https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/CENV6%22

Feakin, T, 2013, *Enter the cyber dragon*, Australian Strategic Policy Institute. Retrieved from Enter the Cyber Dragon: Understanding Chinese Intelligence Agencies' Cyber Capabilities (ethz.ch)

Feakin, T, 2016a, *Matching rhetoric with action: Cyber and the 2016 Defence White Paper*, The Strategist, Australian Strategic Policy Institute. Retrieved from Matching rhetoric with action: cyber and the 2016 Defence White Paper | The Strategist (aspistrategist.org.au)

Feakin, T, 2016b, *Prioritising cyber between strategic partners – The U.S.-Australia cyber dialogue*, Center for Strategic and International Studies, International Cyber Policy Centre, Australian Strategic Policy Institute. Retrieved from 161020_Australia_US_Cyber_Security_Dialogue_Readout.pdf (csis-website-prod.s3.amazonaws.com)

Feakin, T, 2017, *Australia's International Cyber Engagement Strategy: Consequences in cyberspace*, The Strategist, Australian Strategic Policy Institute. Retrieved from Australia's International Cyber Engagement Strategy: consequences in cyberspace | The Strategist (aspistrategist.org.au)

Fischerkeller, M & Harknett, R, 2017, *Deterrence is Not a Credible Strategy for Cyberspace*, Orbis 61, no. 3, pp. 381-393

Fier, J, 2019, *Speed, scale, and scope: A threat analyst's predictions for cyberattacks in 2020*, SecurityWeek, accessed 14/9/23. Retrieved from Speed, Scale, and Scope: A Threat Analyst's Predictions for Cyberattacks in 2020 - SecurityWeek

Filkins, D, 2019, John Bolton on the Warpath, *The New Yorker*. Retrieved from John Bolton on the Warpath | The New Yorker

Finnemore, M, & Sikkink, K, 1998, International norm dynamics and political change, *International Organization*, vol. 52, no. 4, pp. 887–917.

FireEye, n.d., *Advanced persistent threat groups*, accessed 31 January 2019. Retrieved from https://www.fireeye.com/current-threats/apt-groups.html

FireEye, 2015a, *Threat research: Demonstrating hustle, Chinese APT groups quickly use zero-day vulnerability (CVE-2015-5119) following hacking team leak*, accessed 15/10/2019. Retrieved from https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html

FireEye, 2015b, *Threat research: Operation Clandestine Wolf – Adobe Flash zero-day in APT3 phishing campaign*, accessed 15/10/2019. Retrieved from https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

FireEye, 2017, 6 April, *APT10 (MenuPass group): New tools, global campaign latest manifestation of longstanding threat*, accessed January 31, 2019. Retrieved from https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html.

FireEye, 2018, 13 September, *APT10 targeting Japanese corporations using updated TTPs*, accessed January 31, 2019. Retrieved from https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

Fitzgerald, B, 2015, *Australia needs calibrated deterrence against cyber attacks*, theinterpreter, accessed 13/5/2022. Retrieved from https://www.lowyinstitute.org/the-interpreter/australia-needs-calibrated-deterrence-against-cyber-attacks

Ford, S, 2018, *The ethics of 'securitising' cyberspace*, The Conversation. Retrieved from The ethics of 'securitising' Australian cyberspace (theconversation.com)

Foreign Affairs, Trade, and Trade References Committee, 2006. *China's emergence: Implications for Australia.* Senate Printing Unit, Canberra, accessed 4 July 2018. file:///C:/Users/Bryn/Downloads/report_pdf.pdf

Fravel, T M, 2015, China's new military strategy: Winning informationazed local wars, Jamestown, accessed 29 December 2018. Retrieved from https://jamestown.org/program/chinas-new-military-strategy-winning-informationized-local-wars/

Freedman, L, 2004, *Deterrence*, Polity Press, Cambridge, UK.

Frühling, S, 2013, The fuzzy limits of self-reliance: US extended deterrence and Australian strategic policy, *Australian Journal of International Affairs*, vol. 67, no. 1, pp. 18–34.

Gady, F-S, 2016, Are Chinese cyberattacks against US targets in decline?, *The Diplomat*. Retrieved from Are Chinese Cyberattacks Against US Targets in Decline? – The Diplomat

Galloway, A, 2020, Government urged to name and shame countries launching cyber attacks, *The Sydney Morning Herald*, accessed 4/5/2022. Retrieved from

https://www.smh.com.au/politics/federal/government-urged-to-name-and-shame-countries-launching-cyber-attacks-20200721-p55dxl.html

Galloway, A, 2021, 'Illicit gain': Australia accuses China of criminal cyber-attacks, *The Sydney Morning Herald*, accessed 22/02/22. Retrieved from https://www.smh.com.au/politics/federal/illicit-gain-australia-accuses-china-of-criminal-cyber-attacks-20210720-p58b6s.html

Galloway, A, 2022, *From knitting to code-breaking: The life and career of Australia's first female intelligence agency boss*, *The Sydney Morning Herald*, accessed 11/4/2022. Retrieved from https://www.smh.com.au/politics/federal/from-knitting-to-code-breaking-the-life-and-career-of-australia-s-first-female-intelligence-agency-boss-20220408-p5abwm.html

George, A L, & Smoke, R, 1974, *Deterrence in American foreign policy: Theory and practice*, Columbia University Press, New York, NY.

Gertz, B, 2016, *Pentagon links Chinese cyber security firm to Beijing spy service*, The Washington Free Beacon, accessed 9/5/2023. Retrieved from https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/

Gertz, B, 2017, Inside the ring: PLA's hacking hotel, *Washington Times*, accessed 5 February 2019. Retrieved from https://www.washingtontimes.com/news/2017/jan/4/inside-the-ring-plas-hacking-hotel/

Gewirtz, J B, 2019, 27 August, China's long march to technological supremacy, *Foreign Affairs*, accessed 1/1/2022. Retrieved from https://www.foreignaffairs.com/articles/china/2019-08-27/chinas-long-march-technological-supremacy

Gilding, S, 2020, *5G choices: A pivotal moment in world affairs*, The Strategist, Australian Strategic Policy Institute, accessed January 31, 2020. Retrieved from 5G choices: a pivotal moment in world affairs | The Strategist (aspistrategist.org.au)

Gompert, D, & Libicki, M, 2014, Cyberwarfare and Sino-American crisis instability, *Survival: Global Politics and Strategy*, vol. 56, no. 4.pp. 7-22

Goodman, W, 2010, Cyber deterrence: Tougher in theory than in practice?', *Strategic Studies Quarterly*, vol. 4, no. 3, pp. 102–135. Retrieved from Cyber Deterrence: Tougher in Theory than in Practice? (af.edu)

Gorman, S, & Barnes, J E, 2011, Cyber combat: Act of war. *Wall Street Journal*. Retrieved from

http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

Graham, E, 2020, *Australia's serious strategic update*, International Institute for Strategic Studies, accessed 17/4/2022. Retrieved from https://www.iiss.org/blogs/analysis/2020/07/apacific-australia-defence-update

Gray, C, 2000, Deterrence in the 21st Century, *Comparative Strategy*, vol. 19, no. 3, pp. 255–261.

Green, A, 2020, *Intelligence committee cancels UK visit amid diplomatic tensions over Huawei policy leak*, ABC News. Retrieved from Intelligence committee cancels UK visit amid diplomatic tensions over Huawei policy leak - ABC News

Greenberg, A, 2019, *The WIRED Guide to Cyberwar*, WIRED. Retrieved from What Is Cyberwar? The Complete WIRED Guide | WIRED

Groch, S, 2021, *Hackers can stop the trains and the lights. But could they start a war?*, *The Sydney Morning Herald*, accessed 17/3/2022. Retrieved from https://www.smh.com.au/national/robots-worms-and-satellites-how-do-you-fight-a-cyberwar-20210407-p57ha5.html

Hagestad, W, 2012, *21st century Chinese cyberwarfare*, IT Governance Publishing, Cambridgeshire, UK.

Handler, S, 2023, *The 5x5 – China's cyber operations*, Atlantic Council. Retrieved from The 5×5—China's cyber operations - Atlantic Council

Hanson, F, 2017, *Secrecy surrouns cyber warfare team in Canberra basement*, Australian Strategic Policy Institute. Retrieved from Secrecy surrounds cyber warfare team in Canberra basement | Australian Strategic Policy Institute | ASPI

Hanson, F, & Uren, T, 2018, *Australia's offensive cyber capability*, Australian Strategic Policy Institute. Retrieved from https://www.aspi.org.au/report/australias-offensive-cyber-capability

Hare, F, 2012, The significance of attribution to cyberspace coercion: A political perspective, *4th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn.

Harel, A, & Benn, A, 2018, *No longer a secret: How Israel destroyed Syria's nuclear reactor*, Haaretz. Retrieved from No Longer a Secret: How Israel Destroyed Syria's Nuclear Reactor - World News - Haaretz.com

Harknett, R J, 1994, The logic of conventional deterrence and the end of the Cold War, *Security Studies*, vol. 4, no. 1, pp. 88–114. https://doi.org/10.1080/09636419409347576

Harknett, R J, 1996, Information war and deterrence, *Parameters*, vol. 26, no. 3, pp. 93–107.

Harold, S W, Libicki, M, & Cevallos, A S, 2016, *Getting to yes with China in cyberspace*, RAND Corporation, Santa Monica, CA.

Hastie, A, 2021, *Enough is enough: China 'named and shamed' by 30 nations over cyber attacks* [Video interview], Sky News, accessed 4/5/2022. Retrieved from https://www.skynews.com.au/opinion/enough-is-enough-china-named-and-shamed-by-30-nations-over-cyber-attacks/video/6be1aae5256ad87cd02d65df1a3aa466

Hawkins, D, & Kimber, J, 2016, 26 August, *Australia's stance on nuclear deterrence leaves it on the wrong side of history*, The Conversation, accessed 2 August 2018. Retrieved from https://theconversation.com/australias-stance-on-nuclear-deterrence-leaves-it-on-the-wrong-side-of-history-64163

Hayden, M V, 2011, The future of things cyber, *Strategic Studies Quarterly*, vol. 5, no. 1, pp. 3–7.

Heanue, S, 2017, *Talisman Sabre: Australian military enacts war in a bid to prepare for 'emerging threats'*, ABC News, accessed 6/4/2022. Retrieved from https://www.abc.net.au/news/2017-07-16/australian-military-prepares-for-emerging-threats-at-war-games/8712028

Hendry, J, 2022a, *Malicious website blocking mandated by govt*, InnovationAus.com. Retrieved from Malicious website blocking mandated by govt (innovationaus.com)

Hendry, J, 2022b, *What to expect from the incoming Labor government*, itnews. Retrieved from What to expect from the incoming Labor government - Strategy - Training & Development - Security - Telco/ISP - iTnews

Herbert, L, 2016, Attribution of Malicious Cyber Incidents: From Soup to Nuts, *Journal of International Affairs*, vol. 70, no. 1, p. 1-57. Retrieved from Attribution of Malicious Cyber Incidents: From Soup to Nuts by Herbert Lin :: SSRN

Herzog, S, 2011, Revisiting the Estonian cyber attacks: Digital threats and multinational responses, *Journal of Strategic Security*, vol. 4, *no.* 2, 49–60. Retrieved from http://www.jstor.org/stable/26463926

Holland, S, & Chiacu, D, 2021, *U.S. and allies accuse China of global hacking spree*, Reuters, accessed 5/5/2022. Retrieved from https://www.reuters.com/technology/us-allies-accuse-china-global-cyber-hacking-campaign-2021-07-19/

Hsiao, R, 2010, China's cyber command?, The Jamestown Foundation, accessed 27 April 2018. Retrieved from https://jamestown.org/program/chinas-cyber-command/

Hunter, F, Impiombato, D, Lau, Y, Triggs, A, Zhang, A & Deb, U, 2023, *Countering China's coercive diplomacy*, Australian Strategic Policy Institute, Canberra. Retrieved from Countering China's coercive diplomacy | Australian Strategic Policy Institute | ASPI

Hurd, I, 2008, 'Constructivism', in Reus-Smit (Ed.), *Oxford handbook of international relations* (pp. 298–316), Oxford University Press, Oxford.

Hurst, D, 2020a, Cyber-attack Australia: Sophisticated attacks from 'state-based actor', PM says, *The Guardian*, accessed 22/02/2022. Retrieved from https://www.theguardian.com/australia-news/2020/jun/19/australia-cyber-attack-attacks-hack-state-based-actor-says-australian-prime-minister-scott-morrison

Hurst, D, 2020b, Hackers linked to China allegedly stole data from Australian defence contractor, *The Guardian*. Retrieved from Hackers linked to China allegedly stole data from Australian defence contractor | Australian politics | The Guardian

Hurst, D, 2020c, Scott Morrison sends China a signal on cyber-attack – but then fears turn into farce, *The Guardian*, accessed 21/01/2022. Retrieved from https://www.theguardian.com/technology/2020/jun/20/scott-morrison-sends-china-a-signal-on-cyber-attack-but-then-fear-turns-into-farce

Hurst, D, 2021, Australia joins allies in accusing China of 'malicious cyber activities', *The Guardian*, accessed 22/02/2022. Retrieved from https://www.theguardian.com/world/2021/jul/19/australia-joins-allies-in-accusing-china-of-malicious-cyber-activities

Hurst, D, 2023, Australia faces 'dystopian' future of cyber-attacks attacking fabric of society, O'Neil says, *The Guardian*. Retrieved from Australia faces 'dystopian' future of cyber-attacks targeting fabric of society, Clare O'Neil says | Australian security and counter-terrorism | The Guardian

Hurwitz, R, 2015, *A call to cyber norms*, American Bar Association, Chicago, IL.

Hutchins, E, Cloppert M, & Amin R, 2011, Intelligence-Drive Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, *Leading Issues in Information Warfare and Security Research*.

Huth, P. K. (1988). Extended deterrence and the outbreak of war. *The American Political Science Review*, vol. 82, no. 2, 423–443. https://doi.org/10.2307/1957394

Inkster, N, 2013a, Chinese intelligence in the cyber age, *Survival*, vol. 55, no. 1, pp. 45–66. https://doi.org/10.1080/00396338.2013.767405

Inkster, N, 2013b, Conflict foretold: American and China, *Survival*, vol 55, no 5, pp. 7–28. https://doi.org/10.1080/00396338.2013.841802

INSIKT Group, 2021, *China-linked Group RedEcho targets the Indian power sector amid heightened border tensions*, Recorded Future. Retrieved from China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions (recordedfuture.com)

INSIKT Group, 2022, *From coercion to invasion: The theory and execution of China's cyber activity in cross-strait relations*, Recorded Future. Retrieved from From Coercion to Invasion: The Theory and Execution of China's Cyber Activity in Cross-Strait Relations | Recorded Future

International Institute of Strategic Studies, 2021, *Cyber capabilities and national power: A net assessment* [Research Paper]. Retrieved from Cyber Capabilities and National Power: A Net Assessment (iiss.org)

Iran builds firewall against Stuxnet computer virus: Minister, 2019, Reuters, accessed 14/3/2022. Retrieved from https://www.reuters.com/article/us-iran-israel-stuxnet/iran-builds-firewall-against-stuxnet-computer-virus-minister-idUSKCN1SM116

Jackman, S, 2021, At 70, most see US alliance as foundation of our security, *The Australian Financial Review*. Retrieved from ANZUS at 70: Most Australians see American alliance as foundation of our security (afr.com)

Janofsky, A, 2021, *Cyber attribution is more art than science. This researcher has a plan to change that*, The Record, accessed 10/5/2022. Retrieved from https://therecord.media/cyber-attribution-is-more-art-than-science-this-researcher-has-a-plan-to-change-that/

Jensen, B, & Valeriano, B, 2019, *What do we know about cyber escalation? Observations from simulations and surveys*, Scowcroft Center for Strategy and Security, Atlantic Council. Retrieved from What_do_we_know_about_cyber_escalation_.pdf (atlanticcouncil.org)

Jervis, R, 1979, Review of *Deterrence Theory Revisited*, by Alexander George and Richard Smoke. *World Politics*, vol. 31, no. 2, 289–324. https://doi.org/10.2307/2009945

Kallberg, J, 2016, Strategic cyberwar theory: A foundation for designing decisive strategic cyber operations, *The Cyber Defense Review*, vol. 1, no. 1, pp. 113–128.

Kania, E, 2015, China: Active defense in the cyber domain, *The Diplomat*, accessed 3/5/2023. Retrieved from https://thediplomat.com/2015/06/china-active-defense-in-the-cyber-domain/

Kania, E. B. (2021). Artificial intelligence in China's revolution in military affairs. *Journal of Strategic Studies*, *44*(4), 515–542. https://doi.org/10.1080/01402390.2021.1894136

Karp, P, 2016, Malcolm Turnbull reveals cyber attacks breached government agencies, *The Guardian*. Retrieved from Malcolm Turnbull reveals cyber-attacks breached government agencies | Cybercrime | The Guardian

Kaspersky, n.d., *What is an advanced persistent threat (APT)?*. Retrieved from What Is an Advanced Persistent Threat (APT)? (kaspersky.com)

Kaspersky Group, 2014, *The epic Turla operation*, SecureList, accessed 17/3/2022. Retrieved from https://securelist.com/the-epic-turla-operation/65545/

Kaspersky Group, 2015, *Equation Group: The crown creator of cyber-espionage*', accessed 9/5/2023. Retrieved from https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage

Kirk, J, 2016, *Confirmed: Leaked Equation Group hacking tools are real*, BankInfoSecurity, accessed 9/5/2023. Retrieved from https://www.bankinfosecurity.com/equation-group-toolset-real-but-was-leaked-a-9344

Kirk, J, 2022, *Optus under $1 million extortion threat in data breach*, BankInfoSecurity. Retrieved from Optus Under $1 Million Extortion Threat in Data Breach (bankinfosecurity.com)

Kleinman, L, 2020, Cyberattacks: Just how sophisticated have they become?, *Forbes*. Retrieved from Cyberattacks: Just How Sophisticated Have They Become? (forbes.com)

Knopf, J W, 2010, The fourth wave in deterrence research, *Contemporary Security Policy*, vol. 31, no. 1, pp. 1–33.

Knopf, J W, 2013, *Rationality, Culture and Deterrence* [Report Number 2013-009], Monterey Institute of International Studies, Monterey, Vermont.

Korzak, E, & Guitton, C, 2013, The sophistication criterion for attribution, *The RUSI Journal* vol. 158, no. 4, pp. 62–68. https://doi.org/10.1080/03071847.2013.826509

Kostyuk, N, Powell, S, Skach, M, 2018, *Determinants of the Cyber Escalation Ladder*, Cyber Defense Review, Retrieved from Determinants of the Cyber Escalation Ladder > The Cyber Defense Review > Article View (army.mil)

Kozlowski, A, 2015, *The 'cyber weapons gap.' The assessment of the China's cyber warfare capabilities and its consequences for potential conflict over Taiwan*, University of Lodz. Retrieved from The 'Cyber Weapons Gap.' The Assessment of the China's Cyber Warfare Capabilities and Its Consequences for Potential Conflict over Taiwan - CORE

Lapham, J, 2022, *Cyber Security Minister Claire O'Neil flags multiple reforms to protect personal data after Medibank data leaks*, The ABC. Retrieved from Cyber Security

Minister Clare O'Neil flags multiple reforms to protect personal data after Medibank data leaks - ABC News

Laskai, L, 2017, When China's white-hat hackers go patriotic [Web log post], Council on Foreign Relations, accessed 4/5/2022. Retrieved from https://www.cfr.org/blog/when-chinas-white-hat-hackers-go-patriotic

Layton, P, 2023, *The defence gaps in Australia's emerging grand strategies*, The Strategist, Australian Strategic Policy Institute. Retrieved from The defence gaps in Australia's emerging grand strategies | The Strategist (aspistrategist.org.au)

Lebow, R N, 1985, Conclusions, in N Lebow, R Jervis, & J G Stein (Eds.), *Psychology and deterrence*, John Hopkins University Press, Baltimore, MD.

Lebow, R N, 2005, Deterrence: Then and now, *The Journal of Strategic Studies*, vol. 28, no. 5, pp. 765–773.

Lee, J, 2016, 26 August, *South China Sea: The problems of an ambitious award*, East Asia Forum. accessed 20/12/2021. Retrieved from https://www.eastasiaforum.org/2016/08/26/south-china-sea-the-problems-of-an-ambitious-award/

A, Levite, & J, Lee, 2022, Attribution and characterization of cyber attacks, in *Managing U.S.-China tensions over public cyber attribution*, Carnegie Endowment for International Peace, accessed 10/10/2022. Retrieved from https://carnegieendowment.org/2022/03/28/attribution-and-characterization-of-cyber-attacks-pub-86698#:~:text=Attribution%20is%20when%20an%20entity,from%20another%20state's%20computer%20networks.

Lewis, J, 2011, *Cyber attacks, real or imagined, and cyber war*, Center for Strategic and International Studies. Retrieved from Cyber Attacks, Real or Imagined, and Cyber War (csis.org)

Lewis, J, 2022, *Creating accountability for global cyber norms*, Center for Strategic and International Studies. Retrieved from Creating Accountability for Global Cyber Norms (csis.org)

Li, J, 2019, *Conflict mediation with Chinese characteristics: How China justifies its non-interference policy*, Stimson. Retrieved from Conflict Mediation with Chinese Characteristics: How China Justifies Its Non-Interference Policy • Stimson Center

Li, J, 2022, China maps out digital government plan to 2035 as Beijing taps technology to improve its overall efficiency and control, *South China Morning Post*. Retrieved from

China maps out digital government plan to 2035 as Beijing taps technology to improve its overall efficiency and control | South China Morning Post (scmp.com)

Li, Z, 2014, *What we know about the Chinese army's alleged cyber spying unit*, CNN. Retrieved from What we know about China's shadowy army unit 61398 | CNN

Liang, Q, & Xiangsui W, 1999, *Unrestricted warfare*, PLA Literature and Arts Publishing House, Beijing.

Libicki, M C, 2009, *Cyberdeterrence and cyberwar*, RAND Corporation, Santa Monica, CA.

Libicki, M C, 2011, The nature of strategic instability in cyberspace, *The Brown Journal of World Affairs*, vol. 18, no. 1, pp. 71–79. Retrieved from http://www.jstor.org/stable/24590777

Libicki, M C, 2014, Why cyber war will not and should not have its grand strategist, *Strategic Studies Quarterly*, vol 8, no. 1, p. 23-39.

Libicki, M C, 2017a, *The convergence of information warfare*, *Strategic Studies Quarterly*, (Spring).

Libicki, M C, 2017b, *It takes more than offensive capability to have an effective cyberdeterrence posture*, RAND Corporation. Retrieved from https://www.rand.org/pubs/testimonies/CT465.html.

Libicki, M C, 2018, Expectations of cyber deterrence. *Strategic Studies Quarterly*, vol. 12, no. 4, pp. 44–57. Retrieved from https://www.jstor.org/stable/26533614

Lindelauf, R, 2021, Nuclear deterrence in the algorithmic age: Game theory revisited, in F, Osinga, & T Sweijs (Eds.) *NL ARMS Netherlands annual review of military studies 2020*. NL ARMS. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-419-8_22

Lindsay, J R, 2015, Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack, *Journal of Cybersecurity*, vol. 1, no. 1, pp. 53–67.

Lonergan, S, 2017, *Cyber power and the international system* (Unpublished doctoral dissertation), School of Arts and Sciences, Columbia University.

Lupovici, A, 2011, Cyber warfare and deterrence: Trends and challenges in research, *Military and Strategic Affairs*, vol. 3, no. 3 p. 49-62.

Lynch, J, & Morrison, E, 2023, *Deterrence through AI-enabled detection and attribution*, Johns Hopkins School of Advanced International Studies, Henry A. Kissinger Center for Global Affairs. Retrieved from Deterrence Through AI-Enabled Detection and Attribution| Johns Hopkins SAIS (jhu.edu)

Lyngaas, S, 2018, *DOJ indictment spotlights China's civilian intel agency – and its hacker recruits*, CyberScoop. Retrieved from DOJ indictment spotlights China's civilian intel agency – and its hacker recruits - CyberScoop

Macklin, D, 2022, Political tensions simmer over Shanghai's COVID-19 crisis, *The Diplomat*, accessed 21/4/2022. Retrieved from https://thediplomat.com/2022/04/political-tensions-simmer-over-shanghais-covid-19-crisis/

Macmillan, J, & Green, A, 2023, *ASIO director tells Five Eyes intelligence summit that alleged Chinese spy was removed from Australia*, The ABC. Retrieved from ASIO director tells Five Eyes intelligence summit that alleged Chinese spy was removed from Australia - ABC News

Maglaras, L, Ferrag, M, Derhab, A, Mukerhjee, M, Helge, J, & Rallis, S, 2018, *Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures*, EAI Endorsed Transactions, accessed 13/10/2022. Retrieved from https://www.researchgate.net/profile/Leandros-Maglaras/publication/328077921_Threats_Countermeasures_and_Attribution_of_Cyber_Attacks_on_Critical_Infrastructures/links/5be336b04585150b2ba6c01e/Threats-Countermeasures-and-Attribution-of-Cyber-Attacks-on-Critical-Infrastructures.pdf

Mandel, R, 2017, *Optimizing cyberdeterrence: A comprehensive strategy for preventing foreign cyberattacks*, Georgetown University Press, Washington, DC.

Mandiant, 2013, APT1: Exposing One of China's Cyber Espionage Units, Report, Digital Publication, available at: https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

Mann, T, 2023, *China hits back over Five Eyes blame for US infrastructure cyber attack*, ABC News. Retrieved from China hits back over Five Eyes blame for US infrastructure cyber attack - ABC News

Mason, M, 2022, The clues that may reveal the Medibank hacker, *The Australian Financial Review*. Retrieved from Medibank data breach: REvil are likely linked to the hack according to these clues (afr.com)

Mason, M, 2023, Chinese hackers use G7 ruse to target Australian government officials, *The Australian Financial Review*. Retrieved from Chinese hackers use G7 ruse to target Australian government officials (afr.com)

Massola, J, 2022, Dreyfus given direct responsibility for cybercrime after Optus hack, *The Sydney Morning Herald*. Retrieved from Optus data breach: Attorney-General Mark Dreyfus given direct responsibility for cyber crime (smh.com.au)

Mattis, P, 2015, *So you want to be a PLA expert?*, War on the Rocks, accessed 1/1/2022. Retrieved from https://warontherocks.com/2015/06/so-you-want-to-be-a-pla-expert/

Mazarr, M J, 2018, *Understanding deterrence*. RAND Corporation. Retrieved from https://www.rand.org/pubs/perspectives/PE295.html

McCaffrie, J, & Rahman, C, 2010, Australia's 2009 Defense White Paper, *Naval War College Review*, vol. 63, no. 1, article 5.

McConnel, M, 2010, Mike McConnel on how to win the cyber war we're losing, *The Washington Post*, February 28, accessed 17/3/2022. Retrieved from https://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

McGuirk, R, 2022, *China envoy says Australia fired first shot with Huawei ban*, APNews, accessed 9/5/2023. Retrieved from https://apnews.com/article/technology-china-sydney-australia-037521cd9d6e09854c98b4acf1acbf20

McKee, A, 2003, *Textual analysis: A beginner's guide*, Sage, London, UK.

McKenzie, N, & Galloway, A, 2020, 31 January, The man who stopped Huawei: A former spook speaks out, *The Sydney Morning Herald*, accessed 1/1/2022. Retrieved from https://www.smh.com.au/national/the-man-who-stopped-huawei-a-former-spook-speaks-out-20200131-p53wi6.html

McKenzie, T, 2017, *Is cyber deterrence possible?*, Air Force Research Institute, Perspectives on Cyber Power, Maxwell Air Force Base, AL.

McKinney, W, 2016, 15 December, *Cyber-deterrence is the future of cybersecurity*, Edgy Labs, accessed 21/12/21. Retrieved from https://edgylabs.com/2016/12/15/cyber-deterrence-future-cybersecurity/

McReynolds J, 2015, *China Brief*, The Jamestown Foundation, vol. 15, no. 8. Retrieved from China_Brief_Vol_15_Issue_12_v2_2.pdf (jamestown.org)

McReynolds J, 2018, *China's strategic support force: A force for a new era*, National Defence University Press, Fort Lesley J. McNair, Washington, DC.

Meacham, S, 2022, *New cyber security centre in Sydney but location remains top secret'* 9News. Retrieved from New cyber security centre in Sydney but location remains top secret (9news.com.au)

Mellado, D, & Rosado D G, 2012, An overview of current information systems security challenges and innovations. *Journal of Universal Computer Science*, vol. 18, no. (12), pp. 1598–1607.

Miao, W, & Lei, W, 2016, Policy review: The Cyberspace Administration of China. *Global Media and Communication*, vol. 12, pp. 337–340. https://doi.org/10.1177/1742766516680879

Microsoft Threat Intelligence, 2018, Out of sight but not invisible: Defeating fileless malware with behavior monitoring, AMSI, and next-gen AV [Web log post], Microsoft Security. Retrieved from Out of sight but not invisible: Defeating fileless malware with behavior monitoring, AMSI, and next-gen AV | Microsoft Security Blog

Microsoft Threat Intelligence, 2023, Volt Typhoon targets US critical infrastructure with living-off-the-land techniques [Web log post], Microsoft Security. Retrieved from Volt Typhoon targets US critical infrastructure with living-off-the-land techniques | Microsoft Security Blog

Moran, N, 2011, Understanding advanced persistent threats: A case study, *login*, vol. 36, no. 4, p. 21-26. Retrieved from https://www.usenix.org/system/files/login/articles/105484-Moran.pdf

Morgan, P M, 2003, *Deterrence now*, University Press, Cambridge.

Morgan, P M, 2010. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* National Research Council, Washington, DC: The National Academies Press. https://doi.org/10.17226/12997

Morresi, E, 2022, Australian election 2022: Labor wins as Greens and independents make major gains [Video report], *The Guardian*. Retrieved from Australian election 2022: Labor wins as Greens and independents make major gains – video report | Australia news | The Guardian

Morton, R, 2022, How it happened: Medibank hack came via a single login, *The Saturday Paper*. Retrieved from How it happened: Medibank hack came via a single login | The Saturday Paper

Motwani, N, 2023, *AUKUS's three pillars of uncertainty: sovereignty, strategy and costs*, The Strategist, Australian Strategic Policy Institute. Retrieved from AUKUS's three pillars of uncertainty: sovereignty, strategy and costs | The Strategist (aspistrategist.org.au)

Mueller, M, Grindal, K, Keurbis, B, & Badei, F, 2019, Cyber attribution: Can a new institution achieve transnational credibility?, *The Cyber Defense Review*, vol. 4, no. 1, pp. 107–122. Retrieved from https://www.jstor.org/stable/10.2307/26623070

Nakashima, E, 2010, *Pentagon considers pre-emptive strikes as part of cyber defense [sic] strategy*, Activist Post. *Retrieved from* Pentagon considers preemptive strikes as part of cyber-defense strategy - Activist Post

Nakashima, E, 2020, NSA found a dangerous Microsoft software flaw and alerted the firm – rather than weaponizing it, *The Washington Post*. Retrieved from NSA found a dangerous Microsoft software flaw and alerted the firm — rather than weaponizing it - The Washington Post

National Cyber Security Centre, 2023, *Russian GRU conducting global brute force campaign to compromise enterprise and cloud environments* [Cybersecurity Advisory], accessed 17/3/2022. Retrieved from https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

Nevill, L, 2015, 3 August, *We're not really under cyber attack*, The Strategist, Australian Strategic Policy Institute, accessed 13 August 2018. Retrieved from https://www.aspistrategist.org.au/were-not-really-under-cyber-attack/

Nevill, L, & Hawkins, Z, 2016, *Deterrence in cyberspace: Different domain, different rules*¸ The Strategist, Australian Strategic Policy Institute. Retrieved from Deterrence in cyberspace: different domain, different rules | The Strategist (aspistrategist.org.au)

Nevill, L, Hawkins, Z & Feakin, T, 2017, *The Australia-US cyber security dialogue*, ASPI. Retrieved from The Australia–US Cyber Security Dialogue | Australian Strategic Policy Institute | ASPI

Newmyer, J, 2010, The revolution in military affairs with Chinese characteristics, *The Journal of Strategic Studies*, vol. 33, no. 4, p. 483-504. DOI: https://doi.org/10.1080/01402390.2010.489706

Newton, C, 2016, 24 October, *Cyber warfare: The new international warfront*, Al Jazeera, accessed 25 October 2016. Retrieved from http://www.aljazeera.com/indepth/features/2016/10/cyber-warfare-international-warfront-161020090216897.html

Ng, J, 2020, China broadens cyber operations, *Asian Military Review*. Retrieved from China Broadens Cyber Options - Asian Military Review

Noble, R, 2020, *Director-General ASD Speech at National Press Club* [Media release], accessed 14/4/2022. Retrieved from https://www.asd.gov.au/publications/director-general-asd-speech-national-press-club

Nye, J, 2017, *Deterrence and Dissuasion in Cyberspace*, International Security, vol. 41, no. 3, p. 44-71.

O'Brien, R, 2022, *The Cyber Defense Index*, MIT Technology Review: Insights. Retrieved from CDIreport.pdf (mittrinsights.s3.amazonaws.com)

O'Neil, C, 2022a, *Expert Advisory Board appointed as development of new Cyber Security Strategy begins*. Retrieved from Expert Advisory Board appointed as development of new Cyber Security Strategy begins (homeaffairs.gov.au)

O'Neil, C, 2022b, *Home Affairs and the long view: National Press Club address*. Retrieved from Home Affairs and the long view - National Press Club Address

O'Neil, C, 2022c, *Launch of the annual cyber threat report* [Press release]. Retrieved from Launch of the annual cyber threat report (homeaffairs.gov.au)

O'Neil, C, 2023, *Latitude financial* [Press release]. Retrieved from Latitude Financial (homeaffairs.gov.au)

O'Neill, P, 2022, *How China built a one-of-a-kind cyber-espionage behemoth to last*, MIT Technology Review, accessed 9/5/2023. Retrieved from How China built a one-of-a-kind cyber-espionage behemoth to last | MIT Technology Review

Ormrod, D, & Turnbull, B, 2016, The cyber conceptual framework for developing military doctrine, *Defence Studies*, vol. 16, no. 3, pp. 270–298.

Osborne, C, 2014, *FBI chief compares Chinese hackers to 'drunk burglars'*, ZDNet. Retrieved from FBI chief compares Chinese hackers to 'drunk burglars' | ZDNET

Otto, G, 2019, *Chinese hackers found and repurposed elite NSA-linked tools*, CyberScoop, accessed 9/5/2023. Retrieved from https://www.cyberscoop.com/china-nsa-hacking-tools-symantec-doublepulsar/

Packham, C, 2019a, *Australia accuses foreign government of cyber-attack on lawmakers*, Reuters, accessed 22/02/2022. Retrieved from https://www.reuters.com/article/us-australia-cyber/australia-accuses-foreign-government-of-cyber-attack-on-lawmakers-idUSKCN1Q704G

Packham, C, 2019b, *Exclusive: Australia concluded China was behind hack on Parliament, political parties – sources*, Reuters, accessed 5/5/2022. Retrieved from https://www.reuters.com/article/us-australia-china-cyber-exclusive-idUSKBN1W00VF

Palmada, B, 2022, *'It wasn't': Cyber Security Minister Clare O'Neil slaps down Optus's claim that it suffered a 'sophisticated' attack*, news.com.au. Retrieved from Optus hack slapdown: Clare O'Neil tells 7.30 attack was not 'sophisticated' | news.com.au — Australia's leading news site

Panda, A, 2016a, 17 September, Japan set to intensify South China Sea involvement, *The Diplomat*, Accessed 21/12/21. Retrieved from http://thediplomat.com/2016/09/japan-set-to-intensify-south-china-sea-involvement/

Panda, A, 2016b, 26 October, Duterte: Settle South China Sea dispute with a little help from Japan?, *The Diplomat*, Accessed 21/12/21. Retrieved from http://thediplomat.com/2016/10/duterte-settle-south-china-sea-dispute-with-a-little-help-from-japan/

Pangburn, D J, 2014, *China's 'Putter Panda' cyber-spies have been hacking the US aerospace industry*, Motherboard, accessed 9/5/2023. Retrieved from https://motherboard.vice.com/en_us/article/78xxxe/chinas-putter-panda-cyber-spies-have-been-hacking-the-us-aerospace-industry

Parameswaran, P, 2015a, 24 October, The limits of Duterte's US-China rebalance, *The Diplomat*, accessed 21/12/21. Retrieved from http://thediplomat.com/2016/10/the-limits-of-dutertes-us-china-rebalance/

Parameswaran, P, 2015b, 16 December, Exclusive: Managing the strained US-Thailand alliance, *The Diplomat*, accessed 21/12/21. Retrieved from http://thediplomat.com/2015/12/exclusive-managing-the-strained-us-thailand-alliance/

Parliamentary Standing Committee on Public Works, 2017, *Report 2-2017: Referrals made November and December 2016*, Commonwealth of Australia, Canberra.

Patacsil, P, 2014, *How the design and evolution of the United States Cyber Command affect its operations* [Research paper no. 1], GMU School of Public Policy. https//doi.org/10.2139/ssrn.2448911

Paul, T V, Morgan, P, & Wirtz, J, 2009, *Complex deterrence: Strategy in the global age*, The University of Chicago Press, IL.

Payne, K B, 2011, Understanding deterrence, *Comparative Strategy*, vol. 30, no. 5, pp. 393–427.

Payne, M, Andrews, K, & Dutton, P, 2021, 19 July, *Australia join international partners in attribution of malicious cyber activity to China* [Media release], Parliament House, Canberra, accessed 11/1/2022. Retrieved from https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china

Pearson, N, 2022, *Government announces team to 'hack the hackers' after Medibank cyber attack*, 9News. Retrieved from Government announces team to 'hack the hackers' after Medibank cyber attack (9news.com.au)

Peltier, T, 2005, *Information security risk analysis*, Auerbach, Boca Raton, FL.

Perloth, N, & Sanger, D, 2019, E.S. escalates online attacks on Russia's power grid, *The New York Times*, accessed September 6, 2023. Retrieved from U.S. Escalates Online Attacks on Russia's Power Grid - The New York Times (nytimes.com)

Perloth, N, & Sanger, D, 2021, China breached dozens of pipeline companies in past decade, U.S. says, *The New York Times*, accessed 2/5/2022. Retrieved from https://www.nytimes.com/2021/07/20/us/politics/china-hacking-pipelines.html

Philbin, M, 2013, *Cyber deterrence: An old concept in a new domain*, Strategy Research Project, US Army War College, Philadelphia, PA. Retrieved from https://nsarchive.gwu.edu/sites/default/files/documents/4344891/United-States-Army-War-College-Cyber-Deterrence.pdf

Phillips, A, 2012, *The asymmetric nature of cyber warfare*, USNI News. Retrieved from The Asymmetric Nature of Cyber Warfare - USNI News

Phillips, T, 2013, Unit 61398 – the featureless 12-storey building which houses one of the world's most dangerous and secretive cyber-hacking operations, T*he Sydney Morning Herald*, accessed 9/5/2023. Retrieved from https://www.smh.com.au/technology/unit-61398--the-featureless-12storey-building-which-houses-one-of-the-worlds-most-dangerous-and-secretive-cyberhacking-operations-20130220-2eqj4.html

Plis, M, 2021, *Top 10 countries where security hackers come from & their types*, Cyberkite. Retrieved from Top 10 countries where security hackers come from & their types | Cyberkite blog

Potkin, F, & Geddie, J, 2023, *The Chinese groups accused of hacking the US and others*, Reuters. Retrieved from The Chinese groups accused of hacking the US and others | Reuters

Price, M, & Uren, T, 2018, *The Debate Papers: Can Australia be a cyber power?* United States Studies Center, Retrieved from The Debate Papers: Can Australia be a cyber power? | United States Studies Centre (ussc.edu.au)

Qiao, L, & Wang, X, 1999, *Unrestricted Warfare*, PLA Literature and Arts Publishing House, Beijing, available at: Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui.pdf (archive.org)

Radware, 2024, *Botnet definition: What is a botnet and how does it work?*. Retrieved from What Is a Botnet and Its Functionality? | Radware

Ramsdale, A, Shiaeles, S, & Kolokotronis, N, 2020, A comparative analysis of cyber-threat intelligence sources, formats and languages, *Electronics*, vol. 9, article 824. https://doi.org/10.3390/electronics9050824

Ranger, S, 2019, *Cyberwarfare escalation just took a new and dangerous turn*, ZDNet, accessed September 6, 2023. Retrieved from Cyberwarfare escalation just took a new and dangerous turn | ZDNET

Rhodes, E, 2000, Conventional deterrence, *Comparative Strategy*, vol. 19, no. 3, pp. 221–253.

Rid, T, 2012, Cyber war will not take place, *Journal of Strategic Studies*, vol. 35, no. 1, pp. 5–32.

Rid, T, & McBurney, P, 2012, Cyber weapons, *The RUSI Journal*, vol. 157, no. 1, accessed 6/3/2022. https://doi.org/10.1080/03071847.2012.664354

Riehle, K, & May, M, 2019, *Human-cyber nexus: The parallels between 'illegal' intelligence operations and advanced persistent threats*, Intelligence and National Security, vol 34, no 2, pp. 189–204, https://doi.org/10.1080/02684527.2018.1534642

Rogin, J, 2012, NSA chief: Cybercrime constitutes the 'greatest transfer of wealth in history', *Foreign Policy*, accessed 9/5/2023. Retrieved from https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/

Ross, R, 2011, *Guide for conducting risk assessments*, National Institute of Standards and Technology, US Department of Commerce, Gaithersburg, MD.

Rossi, S, 2003, *Government goes it alone on security reporting scheme*, ComputerWorld, accessed 28/3/2022. Retrieved from https://www2.computerworld.com.au/article/53292/govt_goes_it_alone_security_reporting_scheme/

Rudd, K, 2011, 15 September, *Joint statement on cyberspace*, accessed 8 August 2018. Retrieved from https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/1095101%22

Rudd, K, 2013, *Opening of the ASIO National Headquarters* [Press release], Department of the Prime Minister and Cabinet, accessed 16/8/2022. Retrieved from https://pmtranscripts.pmc.gov.au/release/transcript-22758

Rudd, K, & Smith, S, 2011, 15 September, *Cooperation on cyber: A new dimension of the US alliance*, accessed 15 December 2021. Retrieved from https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/1095105%22

Ruddock, P, Coonan, H, Nelson, B, & Nairn, G, 2006, *Review of the e-security national agenda* [Media release], accessed 29/3/2022. Retrieved from

https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2FPQ7J6%22

Ryseff, J, 2017, *The maliciously formed packets of August: Cyberwarfare and the offense-defense balance*, Occasional Paper Series, 170907_Ryseff_Cyberwarfare_And_the_Offense_Defense_Balance.pdf (csis-website-prod.s3.amazonaws.com)

Saarinen, J, 2017, *APT 3 Hackers who stole ASIO blueprints linked to Chinese govt*, IT News, accessed 9/5/2023. Retrieved from https://www.itnews.com.au/news/apt3-hackers-who-stole-asio-blueprints-linked-to-chinese-govt-462313

Sadler, D, 2019, *Parliament hack to remain private*, Innovation Aus, accessed 1/1/2022. Retrieved from https://www.innovationaus.com/parliament-hack-to-remain-private/

Sadler, D, 2020, *No surprises: 2020 cyber security strategy*, InnovationAus, accessed 14/4/2022. Retrieved from https://www.innovationaus.com/no-surprises-2020-cyber-security-strategy/

Saltzman, I, 2013, Cyber posturing and the offense-defense balance, *Contemporary Security Policy*, vol. 34, no. 1, pp. 40–63.

Sanger, D E, 2014, 31 August, NATO set to ratify pledge on joint Defense [sic] in case of major cyberattack, *The New York Times*, accessed 21/12/21. Retrieved from http://www.nytimes.com/2014/09/01/world/europe/nato-set-to-ratify-pledge-on-joint-defense-in-case-of-major-cyberattack.html

Sanger, D E, Barnes, J, & Conger, K, 2022, As tanks rolled into Ukraine, so did malware. Then Microsoft entered the war, *The New York Times*, accessed 28/2/2022. Retrieved from https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html

Saukonoko, M, 2021, *Australia prepares for China retaliation after blaming Beijing for Microsoft attack*, 9news, accessed 7/11/2022. Retrieved from https://www.9news.com.au/world/us-blames-china-for-microsoft-exchange-email-server-hack/86210eb5-a4c2-48df-a59e-616a61b0f418

Schmidt, M, & Sanger, D E, 2014, 5 in China army face U.S. charges of cyberattacks, *The New York Times*, accessed 15/3/2022. Retrieved from https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html

Schmitt, M N, 2011, Cyber operations and the Jud Ad Bellum revisited, *Villanova Law Review*, vol. 56, no. 3, article 569. Retrieved from https://digitalcommons.law.villanova.edu/vlr/vol56/iss3/10

Scott, B, 2022, *Australian cyber: What's 'Redspice' for?*, theinterpreter. Retrieved from Australian cyber: What's 'Redspice' for? | Lowy Institute

Scott, B, 2023, *Australia needs to talk more openly about offensive cyber operations*, The Strategist, Australian Strategic Policy Institute. Retrieved from Australia needs to talk more openly about offensive cyber operations | The Strategist (aspistrategist.org.au)

Sear, T, 2019, *The internet is now an arena for conflict, and we're all caught up in it*, The Conversation, accessed 1/1/2022. Retrieved from https://theconversation.com/the-internet-is-now-an-arena-for-conflict-and-were-all-caught-up-in-it-101736

Segal, A, 2015, *Attribution, proxies, and U.S-China cybersecurity agreement*, Council on Foreign Relations, accessed 09/5/2023. Retrieved from https://www.cfr.org/blog/attribution-proxies-and-us-china-cybersecurity-agreement

Seligman, E, 2022, There is no cyber bullet, *Proceedings*, vol. 148, no. 7, Retrieved from There Is No Cyber Bullet | Proceedings - July 2022 Vol. 148/7/1,433 (usni.org).

Shahid, E, 2020, *Cybersecurity needs top priority but is the threat often overexaggerated?*, Alarabiya News, accessed 31/1/23. Retrieved from https://english.alarabiya.net/features/2018/09/21/ANALYSIS-Cybersecurity-needs-top-priority-but-is-the-threat-often-exaggerated-

Sharma, A, 2016, The Triad Theory for strategic cyberwarfare, In, C Samuel & M Sharma (Eds.), *Securing Cyberspace* (pp. 57–80), Institute for Defence Studies and Analysis, New Delhi.

Sheldon, B J, 2012, *State of the Art: Attackers and Targets in Cyberspace*, vol. 14, no. 2, p. 1-19. Retrieved from View of State of the Art: Attackers and Targets in Cyberspace (jmss.org)

Shimshoni, J, 1988, *Israel and conventional deterrence*, Cornell University Press, Ithaca, NY.

Shoebridge, M, 2020, *Defence strategic update promises real change but more is needed*, The Strategist, Australian Strategic Policy Institute, accessed 17/4/2022. Retrieved from https://www.aspistrategist.org.au/defence-strategic-update-promises-real-change-but-more-is-needed/

Shrimpton, B, & Cave, D, 2021, *ANZUS at 70: Technological cooperation: a critical alliance pillar*, The Strategist, Australian Strategic Policy Institute, accessed 18/9/2022. Retrieved from https://www.aspistrategist.org.au/anzus-at-70-technological-cooperation-a-critical-alliance-pillar/

Sigholm, J, & Bang, M, 2013. *Towards offensive cyber counterintelligence: adopting a target-centric view on advanced persistent threats*, Presented at the 2013 European

Intelligence and Security Informatics Conference, Uppsala, Sweden, p. 166-171. Doi: 10.1109/EISIC.2013.37.

Singh, M, 2020, *China's cyber warfare capabilities*, Indian Defence Review. Retrieved from China's Cyber Warfare Capabilities (indiandefencereview.com)

Singh, P, 2023, *Recent Chinese cyber intrusions signal a strategic shift*, The Strategist, Australian Strategic Policy Institute. Retrieved from Recent Chinese cyber intrusions signal a strategic shift | The Strategist (aspistrategist.org.au)

Skopik, F, & Pahi, T, 2020, Under false flag: Using technical artifacts for cyber attack attribution. *Cybersecurity*, vol. 3, no. 8. https://doi.org/10.1186/s42400-020-00048-4

Slay, J, 2022, *Enhancing Australia's national security through ASD's REDSPICE*, Australian Institute of International Affairs, Australian Outlook. Retrieved from Enhancing Australia's National Security Through ASD's REDSPICE - Australian Institute of International Affairs - Australian Institute of International Affairs

Smeets, M, 2022, Why NATO countries don't share cyber weapons [Web log post], National Interest, accessed 16/11/2022. Retrieved from https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/why-nato-countries-don%E2%80%99t-share-cyber

Soesanto, S & Smeets, M, 2021, *Cyber Deterrence: The Past, Present and Future*, Chapter 20 in *Deterrence in the 21st Century, Insights From Theory and Practice*, NL Arms, Netherlands Annual Review of Military Studies

Solomon, M, 2019, 25 July, *Decision fatigue is real – in life and security*, Security Week, accessed 1/1/2022. Retrieved from https://www.securityweek.com/decision-fatigue-real-life-and-security

Speers, D, 2022, *David Speers interview with Minister Clare O'Neil*, *Home Affairs*. Retrieved from https://minister.homeaffairs.gov.au/ClareONeil/Pages/david-speers-interview-minister-clare-oneil-20221113.aspx

Staddon, J. E., & Cerutti, D. T. (2003). Operant conditioning. *Annual Review of Psychology*, vo. 54, pp. 115–144. https://doi.org/10.1146/annurev.psych.54.101601.145124

Stevens, T, 2012, A cyberwar of ideas? Deterrence and norms in cyberspace, *Contemporary Security*, vol 33, no. 1, pp. 148–170.

Stewart, P, 2011, *U.S., Australia to add cyber realm to defense treaty*, Reuters. Retrieved from U.S., Australia to add cyber realm to defense treaty | Reuters

Stilgherrian, 2019, *No such thing as cyber warfare: Australia's head of cyber warfare*, ZDNet, accessed 1/1/2022. Retrieved from https://www.zdnet.com/article/no-such-thing-as-cyber-warfare-australias-head-of-cyber-warfare/

Stilgherrian, 2020, *The disappointment of Australia's new cybersecurity strategy*, ZDNet, accessed 14/4/2022. Retrieved from https://www.zdnet.com/article/the-disappointment-of-australias-new-cybersecurity-strategy/

Stockburger, P, 2017, *Control and capabilities test: Toward a new lex specialis governing state responsibility for third party cyber incidents*, The NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from CyCon_2017_Stockburger.indd (ccdcoe.org)

Stone, J, 2012, Conventional deterrence and credibility, *Contemporary Security Policy*, vol. 33, no. 1, p. 108-123.

Stone, J, 2013, Cyberwar will take place, *The Journal of Strategic Studies*, vol. 36, no. 1, pp. 101–108.

Swinson, M, & Bowe, K, 2022, Why higher penalties for privacy breaches aren't enough, *The Australian Financial Review*. Retrieved from Cyber breaches: Why privacy impact assessments matter (afr.com)

Szeman, J, Skillicorn D B & Leuprecht, C, 2019, 'The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity', *Contemporary Security Policy*, vol. 40, no. 3, pp. 382–407. https://doi.org/10.1080/13523260.2019.1590960

Taddeo, M, 2018, *The Limits of Deterrence Theory in Cyberspace*, Philosophy and Technology, vol 31, no. 3, pp. 339 – 355

Taylor, J, 2022, Medibank confirms hacker had access to data of all 3.9 million customers, *The Guardian*. Retrieved from Medibank confirms hacker had access to data of all 3.9 million customers | Cybercrime | The Guardian

Temple-Raston, D, 2021, *China's Microsoft hack may have had a bigger purpose than just spying*, NPR. Retrieved from Data Stolen in Microsoft Exchange Hack May Have Helped Feed China's AI Project : NPR

The State Council Information Office, 2010, *China's national defense in 2010*. Retrieved from China's National Defense in 2010 (www.gov.cn)

The State Council Information Office, 2015, *China's military strategy*. Retrieved from China's Military Strategy (full text) (www.gov.cn)

The State Council Information Office, 2019, *China's national defense in the new era*. Retrieved from Full Text: China's National Defense in the New Era (www.gov.cn)

The State Council Information Office, 2023, *China unveils plan to promote digital development* [Press release]. Retrieved from China unveils plan to promote digital development (www.gov.cn)

Thomas, T, 2014, China's concept of military strategy, *The US Army War College Quarterly: Parameters*, vol. 44, no. 4, pp. 39–48. https://doi.org/ 55540/0031-1723.2968

Thomas-Noone, B, 2016, *Australia's new cyber ambassador*, The Interpreter, The Lowy Institute, accessed 11/4/2022. Retrieved from https://www.lowyinstitute.org/the-interpreter/australias-new-cyber-ambassador

Thomas-Noone, B & Flatgard, B, 2017, *Does cyber deterrence work*?, The United States Studies Centre, accessed 23/12/21. Retrieved from https://www.ussc.edu.au/analysis/does-cyber-deterrence-work

Thompson, J, 2020, *Why cyber attack misattribution is our top election security threat*, GCN, accessed 6/5/2022. Retrieved from https://gcn.com/cybersecurity/2020/10/why-cyberattack-misattribution-is-our-top-election-security-threat/315781/

Thompson, M, 2012, The cyber threat to Australia, *Australian Defence Force Journal*, no. 188pp. 57–70.

Threat Hunter Team, 2019, *BuckEye: Espionage outfit used Equation Group tools prior to Shadow Brokers leak*', symantec, accessed 9/5/2023. Retrieved from https://www.symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit

Tiezzi, S, 2018, US slaps cyberespionage charges on 2 Chinese intelligence officers, *The Diplomat*, https://thediplomat.com/2018/12/us-slaps-cyberespionage-charges-on-2-chinese-intelligence-officers/

Tillett, A, 2022, Chinese hackers step up their attacks, *The Australian Financial Review*, accessed 7/3/2022. Retrieved from https://www.afr.com/politics/federal/chinese-hackers-step-up-their-attacks-20220214-p59wdg

Toulas, B, 2022, *Optus hacker apologises and allegedly deletes all stolen data*, BleepingComputer. Retrieved from Optus hacker apologizes and allegedly deletes all stolen data (bleepingcomputer.com)

Townsend, K, 2019, *The United States and China – A Different Kind of Cyberwar*, Security Week, accessed 9/5/2023. Retrieved from https://www.securityweek.com/united-states-and-china-different-kind-cyberwar

Triggs, A, 2019, *Is Australia too dumb and too China-dependent?*, EastAsiaForum, accessed 6 September 2023. Retrieved from Is Australia too dumb and too China-dependent? | East Asia Forum

Tubilewicz, C, 2010, The 2009 Defence White Paper and the Rudd Government's response to China's rise, *Australian Journal of Political Science*, vol. 45, no. 1, pp. 149–157.

Turnbull, M, 2016a, *Australia's cyber security strategy* [Press release]. Retrieved from Australia's Cyber Security Strategy | Malcolm Turnbull

Turnbull, M, 2016b, *Launch of Australia's cyber security strategy* [Media release], accessed 1/4/2022. Retrieved from https://www.malcolmturnbull.com.au/media/launch-of-australias-cyber-security-strategy

Turnbull, M, 2017, *Offensive cyber capability to fight cyber criminals* [Media release], accessed 25/3/2022. Retrieved from https://www.malcolmturnbull.com.au/media/offensive-cyber-capability-to-fight-cyber-criminals

Tzu, S, 1963, *The art of war* (S B Griffiths, Trans.), Oxford University Press, Oxford.

United Nations General Assembly, 2010, *Resolution 64/211: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*, 21 December 2009. Retrieved from https://undocs.org/A/RES/64/211

Uren, T, 2020, *Australia's cyber security strategy*, RUSI, accessed 13/4/2022. Retrieved from https://rusi.org/explore-our-research/publications/commentary/australias-cyber-security-strategy

US Department of Justice, Office of Public Affairs, 2004, *Australian computer crime and security survey 2004*, accessed 5/8/2022. Retrieved from https://www.ojp.gov/ncjrs/virtual-library/abstracts/australian-computer-crime-and-security-survey-2004

US Department of Justice, Office of Public Affairs, 2016, *Chinese national pleads guilty to conspiring to hack into U.S. defense contractors' systems to steal sensitive military information* [Press release]. Retrieved from Office of Public Affairs | Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information | United States Department of Justice

US Department of Justice, Office of Public Affairs, 2018, 20 December, *Two Chinese hackers associated with the Ministry of State Security charged with global computer intrusion campaigns targeting intellectual property and confidential business information*,

accessed January 31, 2019. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

US Department of Justice, Office of Public Affairs, 2019, *U.S charges three Chinese hackers who work at internet security firm for hacking three corporations for commercial advantage* [Press release], accessed 9/5/2023. Retrieved from https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

US Department of Justice, Office of Public Affairs, 2020, *Seven international cyber defendants, including 'APT41' actors, charged in connection with computer intrusion campaigns against more than 100 victims globally* [Press release], accessed 27/4/2022. Retrieved from https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

US Department of Justice, Office of Public Affairs, 2020, *The China initiative: Year in review (2019-20)* [Press release], accessed 2/8/2022. Retrieved from https://www.justice.gov/opa/pr/china-initiative-year-review-2019-20

US Department of State, 2011, *Australia-United States ministerial consultations (AUSMIN) 2011 joint communique* [Media release], accessed 23/8/2022. Retrieved from https://2009-2017.state.gov/r/pa/prs/ps/2011/09/172517.htm

Van der Meer, S, 2016, Defence, deterrence and diplomacy: Foreign policy instrument to increase future cybersecurity, in *Securing Cyberspace* (pp. 95–105), C Samuel & M Sharma (Eds.), Pentagon Press, New Delhi.

Van de Velde, 2023, Cyber deterrence is dead! Long live 'integrated deterrence'!, *Joint Force Quarterly*, vol 2, no. 109, p. 41-50.

Van der Schyff, J, 2023, *AUKUS will redefine government-industry partnerships*, The Strategist, Australian Strategic Policy Institute. Retrieved from AUKUS will redefine government–industry partnerships | The Strategist (aspistrategist.org.au)

Vavra, S, 2019, *How did a Chinese APT get a U.S. hacking tool before it was leaked? Check Point has a theory*', CyberScoop, accessed 9/5/2023. Retrieved from https://www.cyberscoop.com/apt3-nsa-tools-smb-check-point/

Volz, D, 2023, Microsoft email hack shows greater sophistication, skill of China's cyberspies, *The Wall Street Journal*. Retrieved from Microsoft Email Hack Shows Greater Sophistication, Skill of China's Cyberspies - WSJ

Von Clausewitz, C, 1989, *On war*, (H Michael & P Peter Eds., Trans.), Princeton University Press, New Jersey.

Walk, Kerry, 1998, *How to write a comparative analysis*, Accessed 13 February 2017. Retrieved from http://writingcenter.fas.harvard.edu/pages/how-write-comparative-analysis

Waltz, Kh, 1979, *Theory of international politics*, Waveland Press, Long Grove, IL

Wang, K, Woetzel, L, Seong, J, Manyika, J, & Chui, M, 2017, *Digital China: Powering the economy to global competitiveness*, McKinsey & Company. Retrieved from Digital China: Powering the economy to global competitiveness | McKinsey

Walker, W, 2000, *Policy Analysis: A Systematic Approach to Supporting Policymaking in the Public Sector*, Journal of Multi-criteria Decision Analysis, 9, pp 11-27. DOI: 10.1002/1099-1360(200001/05)9:1/33.3.CO;2-V.

Waterman, S, 2016, *Cyber commander: US not drawing 'red lines' in cyberspace*, Fedscoop, accessed 21/12/21. Retrieved from http://fedscoop.com/cyber-commander-us-not-drawing-red-lines-in-cyberspace

Waters, G, 2008, Protecting information infrastructures, in *Australia and cyber-warfare*, ANU E Press, Canberra.

Waters, G, Ball, D, & Dudgeon, I, 2008, *Australia and cyber-warfare*, Australian National University E Press, Canberra, 0200

Weiduo, S, 2023, China unveils blueprint for propelling digital development through 2035, *Global Times*. Retrieved from China unveils blueprint for propelling digital development through 2035 - Global Times

Weiss, J, 2023, *Don't panic about Taiwan*, Foreign Affairs. Retrieved from Don't Panic About Taiwan | Foreign Affairs

Welburn, J, Grana, J, & Schwindt, K, 2023, Cyber deterrence with imperfect attribution and unverifiable signaling, *European Journal of Operational Research*, vol. 306, no 3, pp. 1399–1416. https://doi.org/10.1016/j.ejor.2022.07.021

Welch, D, Hui, E, & Dziedzic, S, 2020, *Cyber attacks' point to China's spy agency Ministry of State Security, as Huawei payback, say former Australian officials*, ABCNews. Retrieved from 'Cyber attacks' point to China's spy agency, Ministry of State Security, as Huawei payback, say former Australian officials - ABC News

Westbrook, T, 2017, *Joint strike fighter plans stolen in Australian cyber attack*, Reuters, accessed 13 August 2018. Retrieved from https://www.reuters.com/article/us-australia-defence-cyber/joint-strike-fighter-plans-stolen-in-australia-cyber-attack-idUSKBN1CH00F

White, H, 2013, *The China choice: Why America should share power*, Black, Collingwood

Wildi, D, 2023, *Applicability of the* Jus in Bello *to Cyber Operations Against Civilian Data: A Legel Grey Zone in the Protection of Data*, GSI Working Paper, Universite de geneve, Retrieved from BA_LAW_2023-04.pdf (unige.ch)

Williams, C, 2021, China's cyber attacks against Australia should be of great concern, *The Canberra Times*. Retrieved from China's cyber attacks against Australia should be of great concern | The Canberra Times | Canberra, ACT

Williams, D, 2001, *Protecting the National Information Infrastructure*, Parliament of Australia, accessed 28/3/2022. Retrieved from https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/IM446/upload_binary/im4461.pdf;fileType=application%2Fpdf#search=%22media/pressrel/IM446%22

Wilner, A X, 2019, US cyber deterrence: Practice guiding theory, *Journal of Strategic Studies*, vol. 43, no. 2, pp. 245–280.

Wilson, C, 2022, *The Optus hacker is being treated as the real deal by the government. Its apology can't be trusted*, Crikey. Retrieved from Optus data breach: hacker all but confirmed as being behind attack (crikey.com.au)

Winkler, K, 2022, *Budget's $9.9b cybersecurity spending is worth every dollar*, *The Australian Financial Review*, accessed 6/7/2022. Retrieved from https://www.afr.com/politics/federal/budget-s-9-9b-cybersecurity-spending-is-worth-every-dollar-20220330-p5a999

Wirtz, J, 1993, Strategic conventional deterrence: Lessons from the maritime strategy, *Security Studies*, vol. 3, no. 1, pp. 51–117.

Withers, S, 2022, *Australia to spend $9.9bn on intelligence and cyber capabilities*, ComputerWeekly.com, accessed 17/5/2022. Retrieved from https://www.computerweekly.com/news/252515281/Australia-to-spend-A99bn-on-intelligence-and-cyber-capabilities

Wong, P, 2023, *National Press Club Address, Australian interests in a regional balance of power* [Speech], Minister for Foreign Affairs. Retrieved from National Press Club Address, Australian interests in a regional balance of power | Australian Minister for Foreign Affairs (foreignminister.gov.au)

Wroe, D, 2019, China key suspect in pre-election hack against major parties, *The Sydney Morning Herald*, accessed 1/1/2022. Retrieved from https://www.smh.com.au/politics/federal/china-key-suspect-in-pre-election-hack-against-major-parties-20190218-p50ymg.html

Wuthnow, J, 2019, *China's 'New' Academy of Military Science: A revolution in theoretical affairs?*, Jamestown, China Brief. Retrieved from China's 'New' Academy of Military Science: A Revolution in Theoretical Affairs? - Jamestown

Wuthnow, J, 2021, *What I Learned From the PLA's Latest Strategy Textbook*, China Brief, vol 21, no 11, The Jamestown Foundation, available at: https://jamestown.org/program/what-i-learned-from-the-plas-latest-strategy-textbook/#:~:text=Introduction.%20In%20August%202020,%20China%E2%80%99s%20National%20Defense%20University%20(NDU)%20released

Wuthnow, J., & Fravel, M. T. (2022). China's military strategy for a 'new era': Some change, more continuity, and tantalizing hints. *Journal of Strategic Studies*, *46*(6–7), 1149–1184. https://doi.org/10.1080/01402390.2022.2043850

Wuthnow, J, & Saunders, P, 2013, *Chinese military reforms in the age of Xi Jinping: Drivers, challenges, and implications*, National Defence University Press, Washington, DC.

Wyche, L, & Goss, D D, 2016, Attacking cyber: Increasing resilience and protecting mission essential capabilities in cyberspace, *The Cyber Defense Review*, vol. 1, no. 2, pp. 15–19.

Yao, D, & de Soto, B G, 2022, A preliminary SWOT evaluation for the applications of ML to cyber risk analysis in the construction industry, *IOP Conference Series: Materials Science and Engineering*, 1218 012017. https//doi.org/10.1088/1757-899X/1218/1/012017

Yi, Y, 2016, *This paper analyzes the characteristics, types, and key points of deterrence in cyberspace*, CPCnews. Retrieved from A Brief Analysis of the Characteristics, Types and Key Points of Application of Cyberspace Deterrence--Theory-People's Daily Online

Yin, R, 2014, *Case study research: Design and methods* (5th ed.), Sage, Thousand Oaks.

Yip, I, 2020, *Australia's new cyber security strategy is lacking precision when it comes to execution and outcomes*, startupdaily, accessed 14/4/2022. Retrieved from https://www.startupdaily.net/2020/08/australias-new-cyber-security-strategy-is-lacking-precision-when-it-comes-to-execution-and-outcomes/

Young, B R, 2022, North Korea knows how important its cyberattacks are, *Foreign Policy*, accessed 17/5/2022. Retrieved from https://foreignpolicy.com/2022/02/09/north-korea-knows-how-important-its-cyberattacks-are/

Yu, V, 2022, Xi Jinping tells China's army to focus on preparation for war, *The Guardian*. Retrieved from Xi Jinping tells China's army to focus on preparation for war | China | The Guardian

Zaagman, E, 2020, *Cyber sovereignty cuts both ways*, theinterpreter. Retrieved from Cyber sovereignty cuts both ways (lowyinstitute.org)

Zhang, M, 2023, TikTok and beyond: How China's ascendency in digital technology challenges the global order, *The Diplomat*. Retrieved from TikTok and Beyond: How China's Ascendancy in Digital Technology Challenges the Global Order – The Diplomat

Zhou, C, 2020, *China's Communist Party is at a fatal age for one-party regimes. How much longer can it survive?*, ABC News, accessed 19/5/2022. Retrieved from https://www.abc.net.au/news/2020-01-05/chinas-communist-party-is-at-a-fatal-age-for-one-party-regimes/11807138

Zuo, M, 2016, China aims to become internet superpower by 2050, *South China Morning Post*, accessed 21/12/21. Retrieved from http://www.scmp.com/news/china/policies-politics/article/1995936/china-aims-become-internet-cyberpower-2020