# SMALL STATES AND THE STRATEGIC UTILITY OF CYBER CAPABILITIES

by

FRANCIS RICO C. DOMINGO

A thesis submitted to for the degree of
DOCTOR OF PHILOSOPHY

School of Politics and International Relations
University of Nottingham
July 2018

# Abstract

The information revolution has profoundly influenced the interaction between states in the twenty-first century. Networked computers have supported the operations of the global financial system, industrial services, and even the conduct of military operations. Due to this revolution, the level of dependence on networked technologies has risen exponentially following the evolution of the Internet. However, networked technologies have also exposed vulnerabilities that have been exploited by hostile actors to disrupt systems, infiltrate networks, and aggravate conflicts.

While the academic literature on cybersecurity has substantially increased in the past decade, most scholars have focused their attention on the capabilities of great powers and strategic behaviour in cyberspace. Despite the cyber incidents involving Estonia and Georgia, as well as the proliferation of cyber capabilities among states, scholars have continued to overlook the relevance of small states in cyber interactions. The significance of this research gap is more prominent in the studies on the Asia-Pacific Region where a substantial amount of studies have focused on the foreign and security strategies of small states but very few have focused on the cyber dimension.

This research gap is addressed by the study by exploring the strategic utility of cyber capabilities for small states in the region. More specifically, it addresses the puzzle: *Why have small states developed cyber capabilities despite its obscure strategic value?* On this, three additional questions are considered: What factors influence the development of cyber capabilities? What are the advantages and limitations of developing cyber capabilities? What are the implications of cyber capabilities on the foreign and security policies of small states?

The primary objective of the study is to develop a more comprehensive understanding of the strategic utility of cyber capabilities as foreign policy instruments for small states. It hypothesises that two necessary conditions influence the development of cyber capabilities in small states: the balance of power in the Asia-Pacific (primary condition) and strategic culture (secondary condition). The interplay between these two conditions provides a stronger explanation regarding why small states develop cyber capabilities regardless of the ambiguity surrounding the strategic utility of cyber capabilities. Based this hypothesis, it draws on neoclassical realism as a theoretical framework to account for the interaction between systemic and the domestic variables. The study also pursues three secondary objectives. First, it aims to determine the constraints and incentives that affect the development of cyber capabilities. Second, the study evaluates the functionality of these cyber capabilities for small states. Lastly, it assesses the implications of cyber capabilities on the military strategies and foreign policies of selected small states.

# Acknowledgements

This thesis is a product of my experiences and ideas that I gathered during my engagements in academia, government, and the private sector. The idea of studying the convergence of technology and politics was first introduced to me by Brig. Gen. Nicolas D. Ojeda Jr. (ret.) and Kathline Tolosa who assigned me to assess the cybersecurity efforts on the government during my work with the Armed Forces of the Philippines in 2010. I thank Ren Delos Santos for convincing me about the strong potential of cybersecurity as a postgraduate research topic.

The research proposal for thesis was written under the guidance of Professor Colin Gray and Dr. Geoffrey Sloan during my studies at University of Reading. My experience in Reading provided me with the intellectual foundation and curiosity in Strategic Studies that enabled to me to cope with the complexities of studying military and strategic affairs. I am thankful to Dr. Kenton White for his insights about research methods and the interplay between strategy and technology.

In completing the thesis, I had the privilege of meeting different people that enriched my experiences and enabled me to move forward in my research. I gained invaluable insights about doing fieldwork in Asia-Pacific from Professor Lorraine Elliot who was a Highfield Fellow during my first year of PhD studies. She was instrumental in connecting me to people across the region. In New Zealand, I am really grateful for the assistance and advice of academics and staff at Victoria University Wellington: Professor Robert Ayson, Dr. David Capie, Pennie Gapes, and Jonette Crysell. I thank Gaylene Preston for her hospitality and "coolness" in accommodating my stay in Wellington. My fieldwork in Singapore was demanding but productive thanks Dr. Alan Chong, Joseph S. Franco, Anthony Lim, Dr. Bernard Loo and Thaemar Tana. I am thankful to Bons and Mayet Yuhico for the generosity and experiences they shared during my stay in Singapore.

My experience at Nottingham was very pleasant thanks to the different people I had the privilege of interacting with. I am thankful to my batchmates, Annabelle de Heus, Dishil Shrimankar, Ibtisam Ahmed, Dun Mao, Abdul-Jalilu Ateku, May Pei Lee, Hong Hieu Huynh, Suyani Indriastuti, and Maria Burczynska for sharing the burden and challenges of pursuing a PhD. I thank Dr. Carole Spary, Professor Wyn Rees, and Dr. Bettina Renz for taking time to review several chapters my thesis. I thank Professor Katharine Adeney for supporting my PhD fieldwork and Professor Steve Fielding for making our postgraduate experience more dynamic. Dr. Pauline Eadie was responsible for my transfer to University of Nottingham so I will always be thankful for her persistence. I am grateful to my examiners, Dr. Madeline Carr and Dr. David Gill for thoroughly reviewing my PhD thesis and engaging in a difficult but very constructive discussion about my work.

My supervisors, Dr. Rory Cormac and Dr. Andrew Mumford, were instrumental in making my academic experience in Nottingham exceptional. I am very grateful for the experiences they shared, the expertise they offered, and the high standards they demanded throughout the supervision process. Rory and Andrew are exemplary academics that PhD students should strive to emulate. My work in academia would not be possible without the support of Professor Julio Teehankee and Dr. Charmaine Misalucha-Willoughby. Professor Teehankee recruited me into academia and Dr. Willoughby has been my "unofficial mentor" since the start of my academic career.

My postgraduate studies in Nottingham would not have been possible without the tremendous support of my family. I am indebted to my parents for doing the unthinkable and investing extensive resources to allow me to pursue PhD studies. I thank my siblings and my in-laws for sharing my enthusiasm for research and teaching. Most importantly, I express my deepest gratitude and appreciation to my wife Izza for selflessly supporting my academic career and transcending the sacrifices that come with it.

# List of Tables and Figures

# Table of Contents

# Chapter 1
## Introduction: Small States and Cybersecurity

The information revolution has profoundly influenced the interaction between states in the twenty-first century. Networked computers have supported the operations of the global financial system, industrial services, and even the conduct of military operations. Due to this revolution, the level of dependence on network-enabled technologies has risen exponentially during the past decade (Carr, 2016, pp. 1-2). This phenomenon however, has also led to precarious national security concerns as different hostile actors have exploited the ubiquity of cyberspace to disrupt information, infiltrate networks, and aggravate conflicts. These threats have continued to generate debates within academic and policy circles regarding the development of appropriate strategies for securing cyberspace.

The necessity of understanding the dynamics of cyber interactions before developing and prescribing strategies to mitigate cyber conflict have been emphasised by several scholars of International Relations. One perspective contends that the Internet is not useful for the execution of political conflict because it cannot function as the final arbiter of physical violence (Gartzke, 2013, p. 72). Another perspective stresses the sizable empirical gap between a constructive analysis of critical international processes and the actual assessment of cyber interactions (Valeriano and Maness, 2015, p. 45). A third view argues for the need to develop established interpretations of cyber phenomena since it involves analysis of new experiences that existing theories may be unable to clarify (Kello, 2013, 7-8). Lastly, there is also a contention that prevailing theoretical paradigms such as realism, liberalism, and constructivism are out of date and cannot account for cyber interactions since these theories were "superseded by novel ideas and critical reframing during the latter decades of the century" (Choucri, 2012, pp. 15-16).

Policymakers on the other hand, have prioritised the development of cyber capabilities without the benefit of compelling empirical evidence (Valeriano and Maness, 2015, pp. 14-15). For example, former United States (U.S.) Deputy Secretary of Defence, William Lynn (2010, p. 101) argues for the inevitability of military cyber operations: "Although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, air, and space. As such, the military must be able to defend and operate within it." In response to the increasing number of cyber incidents against South Korea, former President Park Geun-hye pledged to develop an "active pre-emptive deterrence strategy", which entails the development of offensive cyber capabilities to strengthen the nation's posture against adversaries in cyberspace (Akutsu, 2013; Keck, 2014; Kim, 2015).

The significance of cybersecurity in maintaining the single digital market has also been a critical issue for the European Union because weak responses to widespread ransomware attacks such as NotPetya and WannaCry may result in consumers losing confidence, businesses losing money, and even the compromise of national security systems (Ansip, 2017). Furthermore, the need for cyber capabilities is also emphasised in the United Kingdom (UK): "In response to the growing cyber threat, we are developing a full-spectrum military cyber capability, including a strike capability, to enhance the UK's range of military capabilities" (Hammond, 2013). Recognising this trend, there are currently more than 40 states that have developed military-oriented cyber strategies and almost 70 states with civilian-oriented cyber strategies (Lewis and Neuneck, 2013, p. 1).

Despite the increasing debates about cyber conflict, there has been no clear policy direction and scholarly consensus on the strategic utility of cyber capabilities as well as the use of computer network operations as part of the foreign policy strategy of states (Gray 2005, pp. 325-326). The gap between the interpretation of policymakers and academics has generated debates about the strategic utility of cyber operations. Policymakers consider the significant potential of exploiting cyberspace for military operations while downplaying the vulnerabilities generated by increased dependence on networked-enabled technologies. Academics on the other hand, point out that while networked-enabled technologies provide more strategic options for states, the utility of cyber capabilities should not be overstated. Three key assumptions underpin the debate on cyber capabilities: asymmetric advantage, offence dominance, and the inapplicability of deterrence (Lynn, 2010; Nye, 2011).

The first core assumption is that asymmetric nature of cyber capabilities allows weaker actors to counter the military advantages of stronger adversaries. While some policymakers highlight the advantages of employing cyber capabilities in military conflicts, these ideas are mostly applicable for powerful states. A strong counterargument against this assumption is that cyber capabilities cannot achieve strategic effect unless supported by considerable government resources and operational capabilities therefore diminishing the asymmetric advantage of weaker states (Betz, 2012, p. 695). This assertion is based on the fact that the most sophisticated cyber operation to date, *Operations Olympic Games*, required a substantial amount of resources in addition to a strong intelligence network to inflict physical damage on an Iranian uranium enrichment facility. A second counterargument argument is that because of its inherent nonphysicality, cyber capabilities should be considered as an enabler of joint military action, instead of an independent means of standalone military action useful for coercive strategic effect (Gray, 2013, p. 54). Based on this argument, it is useful to consider cyber capabilities as supporting instruments because they cannot achieve conquest or independently coerce enemies into complying with the preferences of the attacking state (Gartzke, 2013, pp. 72-73).

A third counterargument offers a fundamental critique against the idea of cyberspace as a domain for warfare. Libicki (2012) contends that it is misleading to think of cyberspace as a warfighting domain because it functions differently from traditional domains of warfare - land, sea, and air. For instance, the concept of domain superiority or the idea that power can prevent rivals from engaging in anything consequential is not applicable to cyberspace because this environment is not unitary, opponents are not clearly identified, and the number of actors involved in a conflict can also be ambiguous. (Libicki, 2012, pp. 332-333). Considering these arguments, it is appropriate to evaluate the validity of the asymmetry assumption for small, less powerful states precisely because they have limited resources and influence in the international system. The study engages with these debates by exploring why small states have developed cyber capabilities as well as the utility of these capabilities as a tool for foreign policy in the Asia-Pacific Region. If cyber capabilities are indeed revolutionary tools that empower the weak then these capabilities can potentially alter the foreign policy interactions between states.

The second core assumption is that cyberspace is offence dominant. Offence dominance refers to the relative ease of conquest against targets (van Evera, 1998, p. 5). A number of policymakers are convinced that asymmetry between weak and strong actors is intensified by the relative ease of attacking networks of adversaries compared to defending against attacks (Lynn, 2010; Panetta, 2012; Alexander cited in Aftergood, 2013; Mullen cited in Zenko, 2015). From a technical perspective, offensive measures seem to be easier than defensive measures because the attacker can vary vectors and signatures faster than the defender can detect and close them (Lindsay, 2013, pp. 375-376). In terms of resources, offence seems to have the advantage as some policymakers are concerned with the high cost of defence given "a cyber environment in which emerging technologies are developed and implemented before security responses can be put in place" (Clapper cited in Garamone, 2012).

This assumption is problematic because the empirical evidence that supports this premise is weak and still untested. First, assessing the overall offence-defence balance during cyber operations is not feasible given the difficulty of obtaining data about cyber operations (Gartzke and Lindsay, 2015, p. 343). Second, offence-defence balance during military operations is typically measured based on several factors such as cumulatively, nationalism, force lethality, force protection, force mobility (Glaser and Kaufmann, 1998, 79-81; Adams, 2003, pp. 52-59). These factors have yet to be applied to the conditions of cyberspace. While Gartzke and Lindsay (2015, p. 346) have reported that attack severity, organizational competence, and actor resolve affects the offence-defence balance in cyber operations, a consensus about these factors has yet to be achieved. Given these considerations, assessing the utility of cyber capabilities for small states is necessary to clarify what networked technologies can actually contribute to the strategy of the less powerful states. While this study does not directly contribute to the debates on the cyber offence-defence balance, it focuses on understanding a more basic aspect of cyber interactions: the purpose of cyber capabilities.

The third core assumption is that deterrence is not effective in cyberspace. Certain policymakers believe that traditional deterrence models of assured retaliation do not apply to cyberspace (Lynn, 2010; Hayden, 2011; Krepinevich, 2012). Deterrence is only possible when enemies are fully aware of the military capabilities of a particular state, but cyber capabilities resist such demonstration due to a number of technical and operational reasons (Libicki, 2013, p. vii). Since attribution requires time and resources to achieve, deterrence would be a weak strategy against cyber intrusions (Lynn, 2010, p. 99).

This assumption has also been disputed based on the alternative interpretations of deterrence. One interpretation is by denial; particularly by countering the use of certain classes of cyber weapons that already have existing countermeasures (Denning, 2015, p. 12). A second is to consider existing deterrence mechanisms such as international norms and laws to dissuade state-level aggression and domestic regimes to minimise crime by non-state actors (Denning, 2015, p. 13). A third interpretation is deterrence through the absence of physical attacks. The use of cyber means can be considered as a sign of successful deterrence when other strategic options such an air strike are assessed be too risky and to avoid retaliation or blowback that occurs as a consequence of conventional military and intelligence operations (Lindsay, 2013, p. 398).

A fourth interpretation is deterrence because of interdependence. The indispensability of networked-enabled technologies for communication and business transactions provides opportunities for states to increase interdependence. Since trade and business transactions are conducted through computer networks incessantly, it would be counterproductive for states to conduct network intrusions that disrupt business operations or erase databases because of the considerable economic losses that can occur as a result of these activities.

For example, despite several incidents of cyber espionage between the China and the U.S., economic relations between the two states are still strong because of the importance of trade and industry. There would be serious complications to this beneficial relationship however, if a major cyber attack that involves physical damage occurs to either state (Nye, 2011, p. 33). The complications of deterrence in cyberspace increase the urgency to consider its implications for less powerful states that have limited resources and influence. Deterrence is a strategy for states with formidable military forces therefore the capacity for cyber operations must also be established if states intend to use cyber operations to deter adversaries. This study relates to these debates by looking into the feasibility of cyber deterrence for small states as part of the broader foreign policy instrument of military action.

The persistent disagreements over the interpretation of cyber phenomena raises more questions regarding the value of cyber capabilities for small, less powerful states that are confronted by inadequate material resources but need to survive in a competitive geopolitical environment. Whereas the assumptions that underpin the debate on cyber capabilities have strong potential, these ideas remain untested in the case of small states. In this sense, challenging or validating these core assumptions makes the study distinctive for three reasons.

Firstly, the study assesses whether small states can derive strategic advantages from the perceived benefits of cyberspace. The security policies of small states are observed to be contingent on the actions and preferences of great powers therefore, it is vital to investigate if advanced technology or the option of using cyber capabilities has any influence on small states' security policies. Research on the cybersecurity of small states is emerging but most works in this area focus on examining the responses to cyber attacks and not really on understanding the how technology affects strategy and foreign policy (e.g. Thomas, 2009; Korns and Kastenberg, 2009; Stapleton-Gray and Woodcock, 2011; Chong, 2012; Burton, 2013; Crandall 2014; Gamreklidze, 2014).

Secondly, the study investigates the extent to which cyber capabilities can be used as a foreign policy tool by small states. Recent research on cybersecurity indicates that great powers such as China, Russia, and the U.S. have been exploiting cyberspace to pursue their foreign policy interests (Valeriano and Maness, 2015). Little is known however, about the cyber strategies of small states. In terms of foreign policy, the literature suggests that the behaviour of small states is different from powerful states due to major differences in population, resources, external influence, and military capabilities among other factors (Handel, 1981; Hey, 2003). Since cyber capabilities have been employed to advance foreign policy interests through espionage, sabotage, and subversion (Rid, 2013, p. xiv), it is crucial to decipher if these functions are applicable to the strategic predicament of small states.

Thirdly, the study evaluates if neoclassical realism can account for the development of cyber capabilities as well as how these support the foreign policies of small states. Prevailing works on cybersecurity are largely policy-oriented and do not engage with theories of International Relations (Dunn Cavelty, 2013). This a key challenge because it is difficult to understand foreign policy strategies and cyber interactions of states without the guidance of prior knowledge that are derived from theories. Moreover, considering that cybersecurity is a new field of inquiry, theory testing is essential to capture the general features of events and processes in ways that emphasise their primary causes (Frieden and Lake, 2005, p. 138). While there are some previous studies that draw on theory, very few of these works consider the significance of small state interactions in cyberspace (Eriksson and Giacomello 2006; Reardon and Choucri, 2012). This scholarship gap underscores the original contribution of the study in the field of International Relations.

## Research Puzzle

The academic literature on cybersecurity has substantially increased in the past decade but most studies have focused on the capabilities of great powers as well as the competition for dominance in cyberspace. Despite the large-scale cyber attacks against Estonia and Georgia and the continuous proliferation of cyber capabilities by weaker states, research on cybersecurity has continued to overlook the relevance of small states in cyber conflicts (Burton, 2013; Areng, 2014). The lack of research on small state cyber engagement is more prominent in studies on the Asia-Pacific Region where academics and security analysts have extensively analysed the behaviour of small states without considering cybersecurity as a foreign policy issue (Goh, 2007; Bitzinger, 2010; Loo, 2009; Lantis, 2014). This scholarship gap is crucial because of two reasons.

First, Asia is considered to be the most active in terms of cyber conflicts. The prevalence of cyber intrusions between states can be attributed the existing geopolitical conditions that are shaped by enduring great power rivalry, territorial disputes, and historical animosities between states (Bitzinger, 2010; Asia: The Cyber Security Battleground, 2013; Tan, 2014; Liff and Ikenberry, 2014). Moreover, the most formidable "cyber powers" in the world - China, North Korea, Russia, and the U.S. – are actively engaged in these geopolitical conflicts and have been proven to employ cyber operations to advance their strategic interests (Wicherski et al., 2011; Lindsay et al., 2015). Since small states are predominantly allied with great powers, increasing cyber conflict may potentially influence small states to consider cybersecurity as a top foreign policy issue (Keohane, 1969; Reiter and Gärtner, 2001).

Second, Asia is home to the largest number of Internet users in the world and has a strong potential to surpass North American and Europe in influence during the next fifteen (Reiber and Sukumar, 2017, p. 9). Since economic, political, and social transactions are increasingly reliant on networked technologies, defending critical networks from intrusions and disruptions is a fundamental aspect of a state's national security in the twenty-first century. In this sense, the use of cyber capabilities to advance foreign policy interests in the region can be instrumental depending on the resources and objectives of a state. While the "cyber powers" can discovering new ways to employ cyber capabilities, little in known about how small states with limited material resources and influence cope with the prevalence of cyber conflict in the region.

This study intends to fill the scholarship gap by examining the strategic utility of cyber capabilities for small states. More specifically, it addresses the puzzle: Why have small states developed cyber capabilities despite its obscure strategic value?  On this, three additional questions are considered: What factors influence the development of cyber capabilities? What are the advantages and limitations of developing cyber capabilities? What are the implications of cyber capabilities on the foreign and security policies of small states?

This study aims to develop a more inclusive understanding of the strategic utility of cyber capabilities for small states.[1] It hypothesises that two necessary conditions influence the development of cyber capabilities in small states: the balance of power in the Asia-Pacific (independent variable/primary condition) and strategic culture (intervening variable/secondary condition). The interplay between these two conditions provides a stronger explanation regarding why small states develop cyber capabilities (dependent variable) regardless of the ambiguity surrounding the strategic utility of cyber capabilities. Following this hypothesis, it draws on neoclassical realism as a theoretical framework to account for the interaction between systemic and the domestic variables. Neoclassical realism posits that the foreign policies of states are predominantly shaped by a predefined geopolitical structure that is bound with the existing constraints within the state (Foulon, 2015, pp. 2-3). The framework therefore acts as an imperfect "transmission belt" between systemic incentives and constraints, on the one hand, and the actual foreign and security policies on the other (Lobell, et al., 2009, p. 4).

Strategic culture is considered an intervening variable in the study because it has been instrumental in supplementing theories focused on national interests

[1] Strategic utility in this study is defined as the contribution of cyber operations to the "course and outcome" of a specific foreign policy issue (Gray, 1996, pp. 163-164).

and the distribution of power (Lantis et. al. 2013). In defining the variable, the study builds on the work of Longhurst (2004): "a distinctive body of beliefs, attitudes and practices regarding the use of force, which are held by a collective (usually a nation) and arise gradually over time, through a unique protracted historical process." Culture is considered as a variable that can influence state preferences but is treated as an "epiphenomenal" or secondary explanation to international systemic constraints (Glenn 2009, pp. 531-533). Consequently, previous studies maintain that research collaboration between both explanatory frameworks has proven to be useful in providing more compelling explanations about strategic preferences of states (Schweller, 2003; Glenn et al. 2004; Dueck 2005).

The study also pursues three secondary objectives. First, it aims to determine the constraints and incentives that affect the development of cyber capabilities. Second, the study evaluates the functionality of these cyber capabilities for small states. Lastly, it assesses the implications of cyber capabilities on the foreign security policy of selected states. These objectives are vital because they address key empirical gaps while contributing towards the development of a more nuanced understanding of why small states develop capabilities.

## Scope and Concepts

The study of cyber phenomena is extensive and involves several fields of inquiry that transcends the social sciences. This study however, is anchored on the field of International Relations and focuses on the state as the primary unit of analysis because it remains the most powerful actor in cyberspace (Nye, 2011). Lindsay (2013, p. 403) notes that states have a dominant role in cyberspace because they "have the most experience managing information system complexity through their trials with combined arms force employment and large-scale systems integration…" Meanwhile, Brantly (2014, p. 465) points out that cyber attacks are a "functional tool of state" since it is capable of influencing "the space between overt diplomacy and overt war." This section defines the scope and fundamental concepts relevant to the study and specifies the characteristics that make cyber capabilities functional foreign policy tools.

In terms of scope, this study considered data on interstate cyber interactions released within the period of 2000 to 2016. This time frame is appropriate because the development of cybersecurity strategies and capabilities started in 2000, while research on consequential cyber incidents such as the *Operation Olympic Games* against Iran in 2009, Snowden revelations in 2013, and intrusions against U.S. Democratic National Convention in 2016 were mostly published during the last four years, making 2016 a valid endpoint for the collection of data (Eriksson and Giacomello, 2006; Reardon and Choucri, 2012; Healey, 2013; Patman and Southgate, 2016; Inkster, 2016).

This study defines cyber capabilities as the ability of a state to access a computer system or network of another state to inflict "damage or harm to living or material entities" (Smeets, 2017, p. 6). In this sense, the utilisation of cyber capabilities is manifested in three types of operations: computer network attack, computer network defence, and computer network exploitation. Computer network attack, a concept that generally signifies offensive actions, is the capability to use computers to "disrupt, deny, degrade, or destroy information" in computers and information systems. Computer network defence, a concept that denotes defensive actions, is the capability to "detect, analyse, and mitigate threats and vulnerabilities, and outmanoeuvre adversaries." Computer network exploitation is the capability to collect intelligence through the use of computer networks to gather data about adversaries (U.S. Department of Defense, 2010).

These operations are considered as general classifications for what states are capable of executing in cyberspace, however the specific operational instrument or weapon involved in executing cyber attacks are designated as "cyber weapons." This study draws on Rid and McBurney's (2012, p. 7) work in defining the concept: a cyber weapon is a computer code that is employed with the intention of "manipulating, threatening or inflicting physical, functional, or mental harm to structures, systems, or living beings." While this definition may be considered outdated and inaccurate because of the difficulty in capturing the precise nature of computer codes, it is adopted in this study because it emphasises the strategic effects of employing a computer code rather than its components or method of attack (cf. Herr and Rosenzweig, 2016, pp. 301-302; Stevens, 2017, pp. 2-3).

In terms of cyber interactions, the study considers cyber power as an extension of politics, which is fundamentally the authoritative allocation of valued things (Easton, 1953, p. 5). This idea is consistent with Choucri's (2012, p. 9) observation: “all politics, in cyber or real arenas, involves conflict, negotiation, and bargaining over mechanisms, institutional or otherwise, to resolve in authoritative ways the contentions over the nature of particular sets of core values.” Since power relates to the allocation of capabilities and resources, the study adopts Nye’s (2011, p. 123) conception of cyber power: “the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain.”

Another concept that is closely related to power is war. While there are several existing definitions of cyber war this study accepts Rid’s (2013) assertion that the concept of war is problematic and even dangerous when applied to cyberspace. An act of war, as Rid (2012, p. 5) maintains, “must be instrumental, political and lethal whether in cyberspace or not.” Since no stand-alone cyber operation on record meets these criteria, the concept of cyber war will not be used in this study. As an alternative, the study follows the work of Valeriano and Maness (2015, p. 32) that suggests the term cyber conflict is more appropriate because it denotes hostile interactions between states but is not necessarily indicative of warfare. Cyber conflict is defined as “the use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities” (Valeriano and Maness 2015, p. 3). Following this definition, the study moves away from a strictly military-oriented understanding of cyber conflict and considers it as a broader foreign policy strategy that states make use of to obtain specific national security objectives  (Valeriano and Maness, 2015, p. 33). Whilst cyber conflict is obviously not limited to interactions between state-level actors, the study examines cybersecurity as a foreign policy issue therefore narrowing the scope of analysis to state interactions, government institutions, and foreign policy strategies.

*Characteristics utilising cyber capabilities*

Previous studies have identified different characteristics that make cyberspace a suitable environment for advancing strategic interests as well as exercising cyber power. For instance, Gray (2013, p. 36) argues that cyber power is different from other geographical domains because it is nonphysical and “cannot compare with the immediate and more lasting harm that nuclear weapons certainly would cause.” Rattray (2009, p. 255) highlights the functionality of cyber power:

"Cyberpower has become a fundamental enabler for the full range of instruments of national power: political, diplomatic, economic, military, and informational." Sheldon (2011) on the other hand, focuses on the stealth as characteristic of cyber power: the "ability to stealthily use cyber power, aided by the inherent difficulties of attributing the identity and motivation of most attackers, makes it a very attractive instrument for governments and other actors." The pervasiveness of cyber power is another characteristic that Sheldon (2013, p. 289) emphasises considering that it can generate strategic effects in each of the other domains "absolutely and simultaneously."

These characteristics are instructive in evaluating the advantages of cyber capabilities as a distinctive tool for foreign policy. Technology is considered a fundamental capability of states that are "made operational but not yet translated into specific instruments" (Brighi and Hill, 2016, p. 162). Cyber capabilities are therefore the actual implementing instruments that states use to influence the behaviour of other states in the international system. In this context, this subsection discusses the unique characteristics of cyber operations by drawing on the four attributes of cyber power: nonphysical, stealthy, functional, and pervasive.

### *Nonphysical*

The first characteristic of utilising cyber capabilities as an instrument to advance foreign policy is that these instruments do not *directly* cause physical damage or harm. The primary instruments used in cyber incidents are cyber weapons or malicious computer codes that are not tangible elements that can cause kinetic damage. This fundamental characteristic defines the nonphysical nature of computer network operations as well as the possible strategic outcomes that cyber operations can achieve.

The nonphysical nature of cyber operations is favourable to powerful states in the region because of two reasons. The first is that the most capable states in terms of cyber operations are rational actors that are not predisposed to instigating war (cf. Goh, 2013, Porter, 2013; Goldstein, 2015). China, Russia, North Korea, and the U.S. may have superior military forces compared to most states in the region but military force is not always a sensible option particularly when responding to foreign policy issues that can lead to further escalation. In this sense, cyber capabilities are useful instruments because these tools can be utilised to disrupt adversaries without inflicting kinetic damage thereby limiting the impact on state interactions.

Employing computer network operations is favourable when the objective is focused on to conveying foreign policy preferences such as North Korea's persistent cyber operations against South Korea or to communicate specific preferences in the context of an existing rivalry such as China's cyber operations against other claimant states in the South China Sea dispute (Wicherski et al. 2011; Jun, et al., 2015; Inkster, 2015). Moreover, since a military response is not a typical response to manage cyber intrusions, these actions are less risky compared other foreign policy measures such as paramilitary operations or maritime intercepts (Gompert and Libicki, 2015; Gompert and Binnendijk, 2016). These considerations can therefore be strong incentives for powerful states to utilise computer network operations to advance their foreign policy interests.

The strategic potential of computer network operations is supported by previous works by Manson (2011), Ayson (2015), Biddle and Oelrich (2016), Saunders and Bowie (2016) confirm that powerful states are employing cyber operations to compete for influence in the region. For instance, Russia and the U.S. have advanced their interest in the region by engaging in several cyber skirmishes that can be classified into two categories: espionage and sabotage. Whereas espionage is a normal occurrence in international relations, Russian intrusions into the U.S. Democratic National Committee and parts of the election infrastructure system is a form of covert action that aims to undermine the political stability of the U.S. (U.S. Office of the Director of National Intelligence, 2017). Furthermore, Russia's proven capability to disrupt power grids through computer network attacks is another indicator of its intention to employ sabotage against its adversaries (Nakashima, 2017). Considering these examples, cyber operations have been advantageous for Russia since it has managed to disrupt a critical political process while provoking a diplomatic rather than a military response from the U.S. (Gambino et al., 2016).

The rivalry between China and the U.S. is another example that has spread into cyberspace, with both states engaged in more than twenty cyber exchanges mostly initiated by China (Lindsay, 2015; Valeriano and Maness, 2015; Segal, 2017). These incidents are mostly characterised as disruption and espionage operations but the persistence and scale of cyber incidents have contributed to the existing tension between the two great powers. A notable incident attributed to the Chinese was *Operation Shady Rat*, a series of coordinated cyber intrusions that targeted forty-nine companies and government agencies in the U.S. from 2006-2010 (Alperovitch, 2011). The intrusions were critical because they compromised the operations of key defense contractors such as Lockheed Martin, Northrop Grumman, and BAE Systems that were involved in the production of the F-35 Joint Strike Fighter in addition to other highly classified U.S. military weapons (US–China Economic and Security Review Commission, 2012, p. 155). The use of cyber capabilities for espionage has been a favourable strategy for China because while the U.S. has responded with its own counter measures, the more definitive response to China's actions has been through diplomacy. Both states have agreed to increase cooperation in countering cybercrime, developing appropriate norms of state behaviour in cyberspace, and establishing mechanisms for high-level joint dialogue on cybersecurity (Collins, 2015). The diplomatic response to serious and extensive cyber intrusions sponsored, directly or indirectly, by China suggests that cyber capabilities are useful for espionage because there is less risk of retaliation and punishment because of the nonphysical nature of cyber operations.

The second reason why nonphysicality is favourable for powerful states is since cyber operations do not inflict kinetic damage, cyber incidents are not automatically considered as military action. This predicament can be exploit and utilised against less powerful states that have limited military capabilities and seek out allies to strengthen their national defence. Ukraine is a key example because it has been a target of at least two significant cyber operations attributed to Russia that left thousands of people without electricity for several hours in 2015 and 2016 (Zetter, 2016; Greenberg, 2017). Despite the gravity of these incidents, there has been no decisive response from Ukraine, great powers such as the U.S. or international institutions such as the North Atlantic Treaty Organisation (NATO) (Giles, 2015). The lack of a decisive response to aggressive but non-kinetic cyber operations encourages powerful states like Russia to exploit this ambiguous area of conflict and continue utilising cyber operations to signal its foreign policy interests to other states. The dynamic behind covert communication using signals will be discussed further in Chapter 4.

There are two implications that can be drawn from this argument. Firstly, it is difficult to justify a case for military action against perpetrators of cyber conflict. The *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013) as well as the findings of the United Nations Group of Governmental Experts in 2013 represent some progress in developing rules for state interactions in cyberspace, but these efforts remain advisory and do not necessarily limit state behaviour (Segal, 2017a). Secondly, regional efforts to establish a code of conduct for cyberspace remain incomplete. For instance, security institutions such as the Association of Southeast Asian Nations (ASEAN) and the ASEAN Regional Forum (ARF) have committed to cooperate in countering cybercrime but there is no clear arrangement that addresses interstate cyber incidents (ASEAN Regional Forum, 2012; Minárik, 2016). In the absence of clear sanctions or consequences for conducting cyber intrusions, states can take advantage of this limitation by conducting cyber operations against rivals in the Region.

*Stealth*

The second characteristic is the stealthy nature of computer network operations. The deployment of cyber weapons is difficult to detect because malicious software can pretend to be legitimate or is integrated within legitimate computer programmes that seem to be non-threatening to users. The stealthy nature of cyber operations is further reinforced by the challenge of attributing cyber incidents.  Attributing intrusions requires time and resources because adversaries can use "multi-stage attacks, where the attacker infiltrates one computer to use as a platform to attack a second, and so on" (Clark and Landau, 2011, p. 27). This method when applied across multiple jurisdictions increases the barriers for discovery thereby making attribution complicated to achieve. An effective strategy for attribution is not straightforward and is dependent on different variables: a range of skills on tactical, operational and strategic levels of analysis, "careful management, time, leadership, stress-testing, prudent communication, and recognising limitations and challenges (Rid and Buchanan, 2013, p. 4). While these complexities can be managed by small states, it will take concerted government effort and extended period for small states to develop the capacity and expertise for proficient attribution.

The surreptitious nature of computer network operations is advantageous for states engaged in rivalries and disputes in the region because these can support intelligence operations against adversaries specifically through espionage and disruption. To be sure, intelligence operations conducted through cyberspace have already been exploited by several states. In terms of espionage, China's capacity for network exploitation is well documented and has proven to be capable enough to infiltrate the most secure networks and collect secret information from various governments. Indeed, interstate cyber conflict is most prevalent in Asia-Pacific partly because of China cyber operations that focus on espionage targeting a range of states  (Deibert, 2009, et al.; Cornish, et al., 2010; Valeriano and Maness, 2015, p. 128; Segal, 2017).

In terms of disruption, North Korea's cyber operations against the U.S. and South Korean interests have been persistent, inflicting DDoS (distributed denial of service) attacks against websites and processes of government agencies, private companies, and civil society groups (Haggard and Lindsay, 2015; Jun, et. al. 2015). A prominent incident involving a U.S.-based company was the network intrusions against Sony Pictures Entertainment (SPE) in 2014. North Korea did not fully succeed in its objective to abandon the release of *The Interview* but it did manage to influence the behaviour of SPE by altering the movie's release, inflicting approximately $80 million worth of damage, and compelling the chief executive to resign (Sharp, 2017, 20). South Korea's case is more problematic since it has been a more frequent target of computer network attacks by its neighbour with at least nine disruptive incidents in since 2009 (Jun*,* et al. 2015). A commonly cited example is the "10 Days of Rain" incident that involved DDoS attacks against multiple targets in South Korea such as media outlets, financial institutions, and government agencies including the website of U.S. Forces Korea (USFK) (Wicherski, et al., 2011). The objective of these attacks was to undermine government services as well as business operations in South Korea, highlighting the geopolitical tension between the two states (Jun et al., 2015).

*Functional*

The third characteristic pertains to the functionality or the range of actions that can be undertaken to support military operations. Cyber operations are functional because these capabilities can enable different military strategies across different domains of warfare (McGuffin and Mitchell, 2014). More specifically, these capabilities contribute to military operations by performing three functions: offensive and defensive operations as well as a transitory function.

One fundamental function of cyber capabilities is defending military networks from cyber operations of adversaries. Modern military command and control systems are managed through digital networks therefore cyber capabilities are necessary to prevent network intrusions and to counter infiltrations that can disorient military operations. Since states are in the process of modernising their military capabilities, securing computers and networks is a fundamental challenge for military forces in the region.

An example of a defensive measure is infiltrating the computer systems of hostile military forces when they breach an air defence identification zone (ADIZ) or operate close to maritime territorial boundaries. An ADIZ "is a designated area of airspace over land or water within which a country requires the immediate and positive identification, location, and air traffic control of aircraft in the interest of the country's national security" (U.S. Federal Aviation Administration cited in Rinehart and Elias, 2015, p. 1). The objective of this measure is to defend a state's sovereignty by dissuading adversaries from operating close to territorial boundaries. This measure can be useful for China's anti-access/anti-denial (A2/AD) strategy in countering U.S. military operations in the region. For instance, Russell (2015, p. 156) suggests that cyber A2/AD operations can be employed against adversaries to "to gain control of the network or infrastructure of cyberspace and manipulate it in such a way as to deny a state the ability to use cyberspace *in any capacity*." In this sense, strategic cyber A2/D2 operations is a realistic strategy that China can use against the U.S. because of its strong dependence on networked technologies. By targeting specific submarine cables and satellites, China can potentially to disrupt or deny the ability of the U.S. to access cyberspace (Dian, 2015; Russell, 2015, pp. 157-162).

Another core function is the use of cyber capabilities offensively by disabling command and control systems during military readiness exercises and maritime operations. The objective of this action is to signal protest or express disapproval over military exercises conducted in contentious areas such as the South China Sea. This measure can be effective because attributing computer network attacks is not straightforward and escalation to conventional military conflict is improbable (Valeriano and Maness, 2015). There has yet to be a confirmed example of cyber incidents against maritime security operations of a state, however the deadly collision between an oil tanker and the naval ship *USS*

*John S. McCain* off the coast of Singapore in 2017 is considered a hypothetical example of cyber operation against naval forces (Groll, 2017). The "steering failure" that contributed to the collision led the U.S. Navy to assess the possibility of a computer network attack against the ships command and control systems (McKirdy, et al., 2017).

Another example of an offensive function of cyber capabilities is the suppression of an adversary's air defence systems by infiltrating and disabling these systems just like the case of *Operation Orchard* in 2007. The Israeli Defence Force enabled the bombing of a Syrian nuclear reactor by infiltrating Syria's military computer networks and manipulating its air defence systems thereby rendering them ineffective (Adee, 2008; Rid, 2013, pp. 42-43). The outcome of the operation was the successful airstrike that destroyed the Al Kibar nuclear reactor that directly contributed Syria's nuclear weapons development.

In addition to supporting conventional operations, another dimension of functionality is the transitory nature of cyber weapons. Transitory in terms of cyber weapons refers to "the temporary ability to access a computer system or network to cause harm or damage to living and material entities" (Smeets, 2017, pp. 5-6). This makes cyber capabilities more functional because unlike conventional military weapons, the effectiveness and impact of cyber weapons decreases relatively quickly because patches can be installed and vulnerabilities closed within an average of 312 days (Smeets, 2017, p. 5). In this context, cyber capabilities are functional mainly for powerful states in the region because while these states are highly vulnerable to cyber intrusions, they have the monopoly of maximising the use of cyber weapons before these reach the "decay period" or the time when effectiveness of cyber weapons rapidly declines due to the discovery of software vulnerabilities by computer vendors (Smeets, 2017, p. 11).

### *Pervasive*

The fourth characteristic is the pervasive nature of cyber operations. Computer network operations take effect in cyberspace and therefore can support military operations in other environments simultaneously and effectively without depleting resources. While military power expressed through land, sea, air, and space can generate strategic effect on each of the other domains, these dimensions of military power cannot sustain concurrent operations because of the risk of resource depletion (Sheldon, 2013, p. 310). The pervasive reach of cyber operations is manifested in the significance of cyber technologies in all sectors of society.

Cyber technologies are fundamental tools for advancing the interests and preserving the national security of states in the twenty-first century. Existing studies suggest that the level of network connectivity achieved by a state correlates with its potential for global competitiveness and economic prosperity (Kvochko, 2013; Bilbao-Osorio, et al., 2014). More precisely, using networks and computers enhances the efficiency and reliability of government processes and transactions with other states. To be sure, high dependence on cyber technologies is one of the main characteristics of advanced economies in the Asia region such as Singapore, Japan, South Korea, Australia, and New Zealand (Bilbao-Osorio, et al., 2014). These advantages together with the necessity to survive in a competitive geopolitical environment have compelled states to make use of cyber operations to protect their national security interests in the ubiquity of cyberspace.

The pervasiveness of cyber operations is also reflected in that these operations can easily affect other sectors such as business and civil society. Whereas conventional military weapons are designed to target hostile military forces, states have limited control over the impact of cyber weapons because they operate in a digital environment that cannot be managed by any state or international institution (Howard, 2015, pp. 26-59; Owen, 2015, pp. 1-21). The case of *Operation Olympic Games* illustrates the challenge in controlling cyber weapons. The Stuxnet worm was successful in disrupting Iran's nuclear production but it also spread to other friendly states including Germany, India, Indonesia, and Pakistan, affecting commercial manufacturing plants that use similar industrial computer control systems produced by Siemens (Porche, 2010; Schneier, 2010; Zetter, 2015). The unintended consequences or collateral damage attributed to the Stuxnet worm raises the issue of accountability and control over malicious software in a digital environment. While it would be very difficult for states in the Asia-Pacific to emulate *Olympic Games*, the operation reveals the political potential as well as the consequences of cyber operations as an instrument of foreign policy (cf. Lindsay, 2013; Slayton; 2017).

*Defining small states*

The focal point of the study is small states. In order to analyse the foreign and security strategies of small states, it is first necessary to define the concept. Ingebritsen et al. (2006) point out that the search for a definition of smallness has driven a wide range of contending debates within the discipline of International Relations. While there is no scholarly consensus on a definition, authors have generally proposed absolute or relative definitions in evaluating smallness. Barston (1973) postulates that there are four possible approaches to defining "small state": population size; objective elements of state capability and placing them in ranking scale; analysing relative influence; identifying characteristics and formulating hypotheses on what differentiates small states from other classes of state. Many authors such as Vital (1967), Inbar and Sheffer (1997), and Ólafsson (1998) make use of absolute numbers as criteria for defining small states, however, this definition has been contested since any precise definition can only be arbitrary (Neumman and Gstohl, 2006).

Keohane (1969, p. 296) offers a definition based on the relative influence of a small state: "a small power is a state whose leaders consider that it can never, acting alone or in a small group, make a significant impact on the system." Elman (1995, p. 171) on the other hand, considers capacity in her definition: "a small state can be defined by its limited capacity to: influence the security interests of, or directly threaten, a great power; and defend itself against an attack by an equally motivated great power." East (1973) and Handel (1981) agree that a combination of variables is a useful set of criteria in defining a small state; these include population, economic capacity and military power. East, however, gives importance to land area while Handel considers influence in the international system as a more appropriate fourth criterion. Crowards (2002) on the other hand, categorises small states based on population, land area and total income.

Recent studies on small states have offered more inclusive but less precise definitions of smallness. Hey (2003) for instance suggests that the definition of a small state is constructed based on perception: "If the state's people and institutions generally perceive themselves to be small, or if other states' peoples and institutions perceive that state as small, it shall be considered." Neumann and Gstohl (2006, p. 6) offers another relative definition: "smallness is a comparative concept: micro-states are smaller than small states, and small states are smaller than middle or great powers but with regard to what and how much?" Finally, Maass (2009, p. 81) does not provide a definition but points out the advantages of the lack of agreement: "…the lack of a consensus definition, has been a significant advantage. It has allowed research to be conducted using a variety of conceptualizations of the small state, adapting and customising definitions to meet particular research needs."

Considering these debates, this study builds on Handel (1981) and Elman's (1995) work and advances a definition that combines absolute and relative criteria for smallness. For the purposes of this study, a small state is characterised by four criteria: a population of less than 10 million; a limited capacity to influence the states within its region; an emphasis on foreign policy issues within its immediate region, and a limited military capability to independently defend itself from an attack by medium or great powers.[2]

Population is selected as a measure for smallness because it is a convenient criterion that approximately represents state size (Maass, 2009, p. 71). In terms of cybersecurity, existing policy reports suggest that the population of a state plays a factor in cyber conflict: "The People's Republic of China (PRC) is home to 1.35 billion people, or more than four times the population of the United States. Therefore, China often has the ability to overwhelm cyber defences with quantity over quality, just as it did in the Korean War and as it might do in any other type of conflict" (Geers et al., 2014, pp. 6-8). Moreover, population is also a strategic resource for building a strong military capability in preparation for cyber conflict: the U.S. Department of Defence needs to "increase the number of cyber warriors . . . [and] scale up efforts to recruit, provide facilities and training, and use these critical people effectively (U.S. Defense Science Board cited in Li and Daugherty, 2015, p. 13). A small population might therefore suggest less capacity to execute and defend against cyber attacks. While Estonia is a prominent case that challenges the significance of population in securing cyberspace, its designation as NATO's multinational and interdisciplinary centre of cyber defence expertise makes it an exception compared to a number of small states that have limited capacity such as Azerbaijan, Belarus, and Georgia

[2] 60 million is the average population of states in the Asia-Pacific Region so states with a population of less than 10 million can be considered as "small" in the context of the region (United Nations, 2017). For distinctions between "great", "medium", and "small" powers see Vellut (1967) and Handel (1981).

(Praprotnik, et al., 2012; Gamreklidze, 2014).

State influence, foreign policy, and military capability were selected as criteria because these variables relate to hard and soft power instruments of states or what Nye (2011, p. xiii-xiv) describes as "smart power." In this sense, a small state's soft power is limited because it lacks the ability to persuade and attract other states to support its political objectives. The foreign policy of a small state would also have a narrow scope due to its limited resources and interests (Hey, 2003). Lastly, in terms of hard power, a small state would have limited military capabilities therefore precluding it from coercing other states to submit to its will as well as defending itself from aggression by more powerful states in the region (Handel, 1981, p. 53).

## Case Selection

*Relevance of small states*

Small states have traditionally played a peripheral role in the construction and maintenance of international security. In adapting to the distribution of power in the international system, these states have tended to pursue reactive security policies, adjusting to the interests of great powers to ensure their own survival (Archer, et al., 2014, 3). The emergence of information and communication technologies (ICTs) however, has created more options for small states to participate in the preservation of global stability and order. In this context, studying the cyber strategies of small states is significant for two reasons.

The first reason is empirically motivated since small states have been constantly involved in cyber incidents. Previous studies suggests a number of small states such as Belarus, Estonia, Georgia, Isarael, United Arab Emirates, and Vietnam were targets of intrusions and denial of service attacks during the past fifteen years (Segal, 2017). While the policy responses of Estonia, Georgia and Israel are well documented, the policy responses as well as the strategies of other small states remain understudied (e.g. Korns and Kastenberg, 2009; Crandall, 2014; Raska, 2015). This gap highlights the relevance of exploring the cyber strategies of highly networked small states that depend significantly on networked technologies, making them vulnerable to cyber intrusions by more powerful states.

The second is theoretically motivated considering that one of the main themes in studying smallness in international relations is through an analysis of material capabilities (Neumann and Gstöhl, 2009, pp. 17-19). Explaining state interactions through capabilities is driven by neorealism, which privileges large states with substantial material capabilities and considers the role of small states to be largely irrelevant. Neorealists who observe small states, have been preoccupied with analysing foreign policy strategies that are shaped by the structure of the international system such as balancing and bandwagoning (Walt, 1987; Wivel, 2008), without considering that small states do not necessarily conform to these behaviours (e.g. Mehdiyeva , 2011; Shlapentokh, 2012; Williams, et al., 2012; Gvalia et al. 2013). Hence, the study draws on neoclassical realism, an alternative version of the theory, which can account for a capability-cantered analysis of small states because it considers both structural and domestic variables in explaining the foreign policy behaviour (Rose, 1998, p. 146) (see chapter 3 for more details on the theoretical framework). Consequently, the study of small states and cyber capabilities becomes more relevant since it contributes to the application of International Relations theory in explaining state interaction through cyberspace.

*Criteria for case selection*

The research study follows the "loose application" of the most similar systems design where there is no systematic match between the cases selected and relevant control variables (Anckar 2007, 389-390). Case selection was based on similarities in *smallness, network readiness, cybersecurity capabilities,* and *geographic location*. The first criterion involves the *smallness* of a state. As discussed previously, this study draws on the work of Elman (1995) and Handel (1981) to develop the definition of *smallness*. In this study, a state is considered "small" if it has a limited population (10 million or less), limited capacity to influence other states within its region (avoids leading military initiatives in the region), limited scope of foreign policy interests (focused only on the Asia-Pacific Region), and limited military capability to defend itself from an attack by a regional power (small military force, small territory, insufficient resources).

Secondly, the states selected have high *network readiness* to develop and sustain the use of cybersecurity capabilities. The study uses the Network

Readiness Index (NRI) developed by the World Economic Forum (WEF) as a basis for measuring each state's network readiness (Bilbao-Osorio et al. 2014). Based on the NRI, states are highly networked if their overall readiness value is at least a 5.4 or higher on a scale of 1 to 7. The score of 1 is assigned to states that have barely utilised network technologies to enhance economic development and well-being while the score of 7 is assigned to states that have maximised the use network technologies to strengthen competitiveness. Although there are very few small states that can actually comply with this measurement, the three states selected all have high network readiness values relative to the states in the Asia-Pacific. Table 1 presents the scores of highly networked states in the Asia-Pacific.[3]

| **State** | **Network Readiness Score** | **Global Rank**<br>(out of 144) |
|---|---|---|
| Singapore | 5.97 | 2 |
| Hong Kong, China | 5.60 | 8 |
| Taiwan, China | 5.47 | 10 |
| Australia | 5.40 | 18 |
| New Zealand | 5.27 | 20 |
| Malaysia | 4.83 | 30 |
| Brunei Darussalam | 4.34 | 45 |

Table 1: States with the highest network readiness scores in the region

Thirdly, the states selected, New Zealand and Singapore, have existing *cybersecurity capabilities* that are confirmed by their respective governments through the publication of an official national cybersecurity strategy. Since the objective is to understand the strategic utility of cybersecurity capabilities of small states, the study would not be feasible if the selected states do not have capabilities. Given this limitation, a negative case is included to strengthen the external validity or generalizability of the cases beyond the context of the study (Bryman, 2012, 47). Specifically, the selection of a negative case (Brunei) is consequential for the study since it conforms to a comparative research design where the scope conditions and assumptions of neoclassical realism are tested against selected small states in the Asia-Pacific (Mahoney and Goertz, 2004, pp. 653-655). Limiting the focus of study to just positive cases or cases that tend to favour the hypothesis, will

[3] These figures are based on the report by Bilbao-Osorio et al. (2014).

contradict the research design and consequently, increase the likelihood of producing invalid conclusions. A more detailed discussion regarding the negative case of the study presented in the subsequent section.

Lastly, the cases were selected based on their *geographic location*. Despite the pervasiveness of cyberspace, existing studies argue that geography continues to be a significant factor in shaping the distribution of power and the foreign policy behaviour of states. Cyberspace, regardless of its unique characteristics, does not transcend geographical constraints since strategic effect or the outcome is still achieved through the exercise of state power in land, sea, air and space (Gray, 1996, pp. 274-276; Lonsdale, et al., 2016, pp. 69-70; Russell, 2017). In this sense, the geographic location is a critical aspect of the study given that a distinctive set of political and security issues affect the Asia-Pacific.

*New Zealand and Singapore as case studies*

New Zealand and Singapore are two of the most highly developed small states in terms of ICT infrastructures and policies in the Asia-Pacific Region (Bilbao-Osorio, 2014, pp. 1-2). Notwithstanding the fundamental differences in their political and economic systems, culture, and historical experiences, the study contends that selection of New Zealand and Singapore is justified on three grounds. First, in terms of politics, both states are oriented towards maintaining an independent foreign policy. While these states actively engage in military activities with different states, they do not have official security alliances with any great power and both consider compliance to preferences of great powers as a constraint to foreign policy (Tan, 2011; Ayson, 2012). In this sense, the cyber strategies of New Zealand and Singapore are important cases to examine because of their conscious effort to manage the foreign influence by cooperating with major powers while still developing national security strategies that primarily reflect their respective national interests.

The second reason has to do with military capabilities. Strategically, the two states have weak military capabilities relative to powerful states in the Asia-Pacific Region. The Singapore Armed Forces (SAF) may be the most advanced in Southeast Asia, but their capabilities are still constrained by Singapore's limited population as well as natural resources. Consequently, these disadvantages have continued to motivate Singapore's inclination towards high-technology conventional capabilities (Huxley, 2004). Meanwhile, the capabilities of the New Zealand Defence Force (NZDF) have been limited due to its government's low priority on defence and lack of material resources (Butcher, 2012). Although the government has allotted considerable funds for capability enhancement, defence affordability remains a significant consideration in modernising the NZDF (New Zealand Ministry of Defence, 2014, p. 18). Studying the cyber strategy of these small states is therefore important because it tests the assumption that cyber capabilities can provide asymmetric military advantages by supplementing the inherent limitations on the military capabilities of New Zealand and Singapore.

The third reason pertains to geopolitical considerations. Geographically, both states are located in the Asia-Pacific, a region characterised by conflict and rivalry (Bercovitch and Oishi, 2010; Wiegand, 2011; Chan, 2013). This point is significant becasue on one hand, a substantial amount of research suggests that cyber incidents occur within the context of political and territorial disputes (Bolt and Brenner, 2004; Gandhi, 2011; Swaine et al., 2015, pp. 57-58; Kallender and Hughes, 2017). Since offline geopolitical conflicts have influenced cyber exchanges between great powers such as China and the U.S., it is not surprising that more secondary states have invested in the development of cyber capabilities in the region (United Nations, 2011, pp. 1-2).

On the other hand, the build-up of the conventional military capabilities is also another established phenomenon in the region (Ball, 2010; Till, 2012). States are enhancing their military forces for various reasons most prominent of which are to adapt to upgrade outdated capabilities and to react to the strategic posture of other states (Bitznger, 2010, Tan, 2014). Since modern military platforms and subsystems are highly dependent on network technologies, having the capacity for computer network operations is essential to protect the integrity of these military systems. It is unclear however, why states like New Zealand and Singapore have taken interest in developing cyber capabilities when they are not directly threatened by adversaries nor have they been targets of any significant cyber incident in the twenty first century. In this context, establishing the link between geopolitics, cyber interactions, and the cyber strategies of small states in the region is another reason why studying these cases can make a relevant contribution to cybersecurity policy and International Relations scholarship.

*Brunei as a negative case*

The selection Brunei as a negative case is based on the logic that it is approximately comparable to New Zealand and Singapore in terms of the selection criteria but its cyber capabilities are not as developed.[4] This logic is based on the Possibility Principle: "Choose as negative cases those where the outcome of interest is possible" (Mahoney and Goertz, 2004, pp. 657-658). Brunei is a relevant negative case because it is also influenced by the distribution of power in the Asia-Pacific (independent variable) but does not have developed capabilities (dependent variable) for computer-networked operations (Lewis and Timlin, 2011, pp. 23-24). Since the positive cases are small states with developed cyber capabilities, testing neoclassical realism using these cases would limit the findings of the study to states with relatively similar characteristics on the dependent variable. Whilst developing wide-ranging generalizations is not the objective of the study, including Brunei as a negative case can provide narrow but useful insights about the value of cyber capabilities for small states.

Brunei is an appropriate negative case in assessing the cyber strategy of small states because the case satisfies the selection criteria of the study but differs in terms of cyber capability development. From a policy perspective, Brunei's independent national cyber strategy does not explain the relevance of cyber threats and, more importantly, does not define the role of the military and security services in securing cyberspace (Haji Mus, 2010). While Brunei's Ministry of Defence has emphasised the importance of computer network defence, it is not apparent that the military has taken any actions to implement this guidance (Feakin, et al., 2015, 21). From an organisational perspective, Brunei does not have an officially recognised agency responsible for implementing a national cybersecurity strategy as well as officially accepted national benchmarking exercises used to measure cybersecurity development (Boyd and Menting, 2015, pp. 106-107). For these reasons, Brunei does not have the same level of cybersecurity maturity as New Zealand and Singapore thus making it a relevant negative case for the study.

[4] Australia, Hong Kong, and Malaysia were not selected because they did not fit the selection criteria of the study. Taiwan was not selected because of its exisiting rilvary with China. Taiwan's rivalry with China contributed to the development of its cyber capabilities (Mulvenon, 2009; Easton et al. 2017).

## Methodology of the Study

Based on an assessment of previous studies, the researcher contends that a comparative research design is the most appropriate research framework for the study for two reasons. First, comparative analysis is a strong design for testing theories, which is one of the key objectives of the study. Burham et al. (2008, p. 68) highlights the benefits of comparison: "Comparative analysis sharpens our understanding of the context in which theoretical problems occur and enables causal inferences to be drawn." Second, quantitative analysis is not feasible because the data about cyber capabilities of most states are not accessible (Liff, 2012, p. 403). Although a pioneering study by Valeriano and Maness (2015) has established that quantitative analysis can provide strong conclusions about cyber interactions, the cases investigated were limited to a specific set of states that are engaged in enduring conflicts or geopolitical rivalries. This sample size excludes a good number of states that are not actively involved in geopolitical conflicts and have the capacity for cyber operations.

Following the comparative design, the study employed three qualitative methods to achieve its objectives. The researcher first used documentary analysis to develop a deeper, more nuanced understanding of the foreign policies and cyber strategies of each state. The data gathered from primary and secondary documents were corroborated by interviews with government officials and cybersecurity analysts from the private sector, think tanks, and the media. Lastly, the method of structured, focused comparison was used to systematically investigate the selected cases and develop general patterns that can be refined into theoretical propositions (Beach, 2012, pp. 238-239).

### *Documentary analysis*

The study mainly relied on primary and secondary sources to examine the foreign policy behaviour and cyber strategies of the selected states. Primary documents were obtained from the following government organizations in New Zealand: Department of the Prime Minister and Cabinet, the Ministry of Defence, the New Zealand Defence Force, and the New Zealand Intelligence Community. In Singapore, documents were sourced from: the Prime Minister's Office, Ministry of Defence Singapore, and the Ministry of Information, Communications and Technology Singapore and the SAF.

A substantial amount of academic literature suggests that documentary analysis is an appropriate method for understanding the workings of states because government documents can provide valuable insights and unique interpretations that are not available from other sources (Rapley, 2008; Bowen, 2009; Johnson and Reynolds, 2005). In using this method, the researcher was aware of the critical issues in applying the method. Quality control is one decisive issue in the assessment of primary documents. The documents were therefore be screened through the following criteria: authenticity, credibility, representativeness and meaning (Scott, 1990, pp. 19-28; Harrison, 2001, pp. 129-132).

The authenticity of a document refers to its genuineness: the substance of a document is consistent with its purpose. Assessing authenticity involve confirming if the document is in its original form and identifying the authors of the document if possible. Establishing credibility required the researcher to understand the context in which the document was produced and the interests that may have driven the author to write the document (Burham et al., 2008, pp. 208-209).

Ensuring representativeness was difficult because this criterion requires that the documents used for the study are "representative of the totality of the relevant documents" (Scott, 1990, pp. 19-28). Since determining the entire universe of relevant documents may not always be possible, the solution to addressing this requirement is focusing on the relevant documents that are officially published and accessible. The last criterion pertains to the meaning or implications of the documents. Documents can only provide a certain amount of information hence; to draw more implications it is necessary for researchers to situate the documents within a context of rigorous analytical and methodological assumptions. Without assumptions, it would be difficult to judge the value of research produced from documentary sources (Burham et al., 2008, pp. 208-209).

Secrecy and access to classified documents are also important issues in documentary analysis. Cybersecurity is considered a sensitive national security issue for states therefore information about cyber capabilities as well as specific details regarding cyber strategies generally are not accessible to the public. Given these limitations, the researcher will focus on obtaining unclassified primary documents that provide empirical evidence about the general direction of the cybersecurity strategies of selected cases. Examples of unclassified documents include defence white papers, national security strategies, defence assessments, military capability plans, agreements on cybersecurity cooperation, national threats assessment, and government reports among others. Collecting these primary documents were feasible because they were uploaded in official government websites and collated as part of the research databases of institutions such as the NATO Cooperative Cyber Defence Centre of Excellence and the Centre for Security Studies at ETH Zürich. Indeed, prior to the field research, the researcher was able to collect a decent number of primary documents relevant to network technology, foreign policy, and military strategy in New Zealand (41 documents), Singapore (30 documents), and Brunei (13 documents).

In addition to unclassified documents, the study will make use of official speeches and correspondence by government officials and agencies as a supplement to documents. These communication documents are also primary sources that can generate insight regarding a state's foreign and security policies that might not be recorded in official documents. Debates regarding defence priorities or the rationale for the enhanced collaboration with the private sector in the area of cybersecurity are examples of issues captured in official speeches and correspondence but not necessarily in documents.

### *Interviews*

The study makes use of interviews as a secondary collection method, to corroborate the documents gathered in New Zealand and Singapore. Interviews are an effective way to obtain information about decision-making process and are particularly useful "whenever it is appropriate to treat a respondent as an expert about the topic at hand" (Leech, 2002, p. 663). The study utilised a semi-structured approach to interviewing government officials, policy analysts, journalists, and technologists. This approach was more useful compared to structured interviews because it enabled more flexibility for following up on whatever aspects are considered important to the study. Moreover, the approach also provides better direction than unstructured interviews since the researcher has a strong control of the organisation and content of the discussion (Brinkmann, 2013, pp. 21-22).

Employing interviews to cross-check primary and secondary documents is consistent with the principle of triangulation, which Bryman (2012, p. 392) defines as "using more than one method or source of data in the study of social phenomena." Triangulation is a vital process in exploring the cyber strategies of the three cases because it strengthens validity by confirming that the conclusions generated are as objective as possible and adding to credibility by reinforcing confidence in the conclusions that are presented (Patton, 2002, 556; Ritchie and Lewis, 2003, pp. 275-276). Berg and Lune (2012, p. 6) interpret this process as "a means of mutual confirmation of measures and validation of findings." The interviews in New Zealand and Singapore therefore focused on verifying: (i) the status of national cyber strategy and implementing government organisations, (ii) the relevance of cybersecurity as a foreign policy issue, (iii) the significance of cyber technologies for the state, and (iv) the presence of research and development on cybersecurity. While these details could have been drawn from government documents, interviews were necessary to validate any variations or contradictions postulated in primary and secondary sources.

Interview participants were selected based on their respective designations in government, private sector, and civil society (see Appendix 1). These sectors are crucial because they are the key drivers that shape the cyber strategies of states (Dunn Cavelty, 2015; Herrick, 2016; Carr, 2016). In terms of process, all interviews were conducted following the practice of informed consent or "a norm which subjects based their voluntary participation in research projects on a full understanding of the possible risks" (Babbie, 2011, p. 69). Participants were therefore encouraged to sign a consent form before proceeding with each interview. In addition, since the participants were more responsive to discussions that were not digitally recorded, most of the interviews were chronicled through detailed note-taking.

The research environment in New Zealand was more conducive than Singapore as demonstrated by the number of participants that volunteered to be interviewed regarding cybersecurity issues. A summary of the interview participants is presented in Table 2 and a more detailed list is presented in Appendix 1. A key factor that differentiates the environment between the two states is their outlook towards national security issues. Managing cyber threats is a top priority for both states but fieldwork confirmed that participants in New Zealand were transparent regarding the discussion of cybersecurity issues because of the low threat environment confronting the state. Indeed, participants did not consider cyber conflict as an imminent or grave threat against the state.

Interviewees in Singapore on the other hand, were less transparent because of the strict government policy against conversations about sensitive national security issues. Participants were mostly guarded and hesitant to discuss the extensive efforts of the state in securing cyberspace. The remedy to manage this barrier was to initially reorient the interview questions to focus on publicly known issues such as responses to data breaches, significance of technology in society, key technology challenges confronting the states, the role of the military in society and then gradually inject key questions that focused on cybersecurity and foreign policy. This adjustment enabled the researcher to collect a modest but sufficient amount of data about Singaore's approach to cybersecurity.

Meanwhile, no fieldwork was conducted in Brunei for three reasons. First, Brunei is treated as a negative case because the state has no dedicated cyber strategy to analyse or even national security strategy that directly addresses cyber threats. Second, primary documents regarding Brunei's digital strategy, although limited in number, were able to provide some concrete insights regarding the general direction of the state's cybersecurity initiatives. Third, it is unlikely that fieldwork would be productive because of the strong government regulation that contributes to lack of public awareness and debate regarding cybersecurity issues (Bilbao-Osorio et al. 2014; Feakin, et al., 2015, 2016).

| State | Government | Private Sector | Civil Society | Total |
|---|---|---|---|---|
| New Zealand | 4 | 3 | 9 | 16 |
| Singapore | 1 | 2 | 7 | 10 |

Table 2: Summary of interview participants per sector

Interviews were not directly used to substantiate the arguments advanced in the study but they were still useful in corroborating other sources of information and clarifying the substance of government documents. There are two reasons for the limited use of interview data. The first is that the information revealed by participants did not depart significantly from the ideas articulated in government documents and private sector reports. While the ideas articulated during the interviews were not just a repetition of what was written, the consistent theme across all interviews was that the cyber strategy is the foundation of the states' efforts to secure cyberspace. In this context, the study prioritised government documents in the event of any contradictions between sources. The second is that the ideas articulated by the participants were useful but not groundbreaking. The information shared by interviewees was certainly crucial for strengthening the validity of the study but there was no exceptional idea that was revealed during field research in New Zealand and Singapore. This is why interview citations are limited and are no extensive quotations drawing on the material collected through interviews.

*Structured and focused comparison*

Since the study examines three cases, the method of structured, focused comparison is appropriate to determine limited inferences and patterns. The method is "structured" in that the researcher collects data on key variables (historical experiences, government security organizations, national security policies) relevant to cyber capabilities and uses the research questions to determine outcomes in the selected cases of the study: New Zealand, Singapore and Brunei. The method is "focused" in that it only includes specific aspects of the cases examined (George and Bennett 2005, 67-72). This method offers two key advantages: conceptual validity and deriving new hypotheses.

Like most social science research, the study also involves variables such as strategic culture that are difficult to measure. This method addresses this issue because it allows the researcher to achieve high levels of "conceptual validity" or to identify and measure the indicators that best represents theoretical concepts (George and Bennett 2005, 20-21). Locke and Thelen (1998) have proven that comparative case studies allow for better "contextualised comparisons" which means that the concepts being compared are "analytically equivalent" even if expressed in different terms across different cases. In the context of the study, contextualised comparison implies that strategic culture, for instance, should be defined and measured in the same manner even if the concept may have different connotations in New Zealand, Singapore and Brunei.

The other advantage of using case studies is discovering new hypotheses. George and Bennett (2005) argue that case studies are useful for identifying new variables and hypotheses. This happened through the course of fieldwork, while examining government documents and during discussions with interviewees in New Zealand and Singapore. Other methods that employ statistical analysis for example, would not maximise these advantages because statistical methods alone cannot provide detailed consideration contextual issues without qualitative analysis and lack distinctive mechanisms for identifying new hypotheses (George and Bennett 2005, pp. 20-21).

## Limitations and Solutions

*Case selection bias*

Selection bias is a common challenge to comparative research designs. It occurs, as Collier and Mahoney explain, "when some form of selection process in either the design of the study or the real-world phenomena under investigation results in inferences that suffer from systematic error" (Collier and Mahoney 1996, pp. 56-60). In practical terms, this bias is manifested when the researcher deliberately selects cases that have extreme values or no variation on the dependent variable.

The researcher argues that selecting on the dependent variable is acceptable for the study because of two important reasons. First, as Dion contends, selection on the dependent variable is acceptable if "there is relatively little data" on the topic (Dion 1998, p. 127; George and Bennett 2005, pp. 20-21; p. 76). Since there are only very few small states that acknowledge possession of cyber capabilities; selection bias is permissible for the study. Second, Collier (1995), Goertz and Starr (2002), and Bennett (2004), have argued that selecting on the dependent variable is useful particularly because it allows the researcher to test whether a variable is necessary for the outcome. This argument supports the objective of the study since it involves examining the conditions for the development of cyber capabilities.

*Lack of representativeness*

The lack of representativeness is a key challenge that confronts the study. The literature on research methods suggests that using case studies would involve the trade-off between achieving high internal validity and good historical explanations of specific cases versus generalisations that apply to broad populations (George and Bennett 2005, 22-25). This challenge is clearly manifested in the study given that the chosen cases are located in the Asia-Pacific where the combination of certain conditions (predominantly low network readiness, competition between great powers, territorial disputes, high occurrence of cyber attacks) are exclusive only to this region in the world. The researcher acknowledges the limitations of using the method and is prepared to sacrifice broad applicability of findings to develop limited conditional generalizations.

Even with this limitation, it is possible that the findings of the study can be applied to other small states beyond the Asia-Pacific Region such Latvia and Lithuania. These states can also be representative cases for two reasons. Firstly, both states face similar geopolitical constraints in Northern Europe considering the assertiveness of Russia towards post-Soviet states, which has increasingly manifested in cyberspace (Gvosdev, 2012; Russell, 2014; Geers, 2015). Secondly, these states satisfy the all selection criteria of the study including cyber capabilities (NATO, 2018).

*Scope conditions and necessity*

Another limitation of case studies is that they can only make tentative conclusions about how much they can generally contribute to the outcomes of specific cases. Case studies are therefore stronger in assessing *whether and how* a variable matters to the outcome, rather than measuring *how much* a variable matters to the outcome of the study (George and Bennett 2005, 25-27). In this regard, the study has addressed this limitation by adjusting the objectives of the study based on what the study can actually prove. Since the study is designed as a theory-testing enquiry, its aims are pragmatic: to demonstrate that other existing theoretical frameworks are inadequate to explain the cyber phenomena and to test the potency and novelty of neoclassical realism in bridging two levels of analysis (system and state) in explaining foreign policy behaviour of small states.

## Organisation of the study

This study explores the cyber strategy of selected small states in six chapters. Chapter 2 identifies the research gaps in the area of International Relations and cybersecurity by evaluating three key themes within the existing literature in these subjects: regional security dynamics in the Asia-Pacific, small states in international relations, and the impact of the information revolution on states. More importantly, the chapter presents the key contributions of the study and explicates how these contributions can address the research gaps in this area of study.

Chapter 3 lays out the theoretical framework of the study in three steps. First, the chapter identifies the levels of analysis involved in the study as well as conceptualises cyber capabilities as a foreign policy instrument of states. Second, it explores the strength of neoclassical realism as a theoretical framework by drawing out relevant themes useful for analysis and comparing the explanatory power of the theory to alternative paradigms used to explain cyber phenomena. Third, it operationalises the framework by discussing the interaction of the variables, observable implications, and limitations. The application of the framework focuses on determining the necessary conditions for the development of cyber capabilities in small states.

Chapter 4 applies the first part of the framework by unpacking the distribution of power as a necessary *primary* condition for the development of cyber capabilities. The chapter argues that relative power distribution in the region is a primary condition because it has a more significant influence on the strategic preference of small states. This system level condition is explored in three phases. The chapter first evaluates the response of selected small states to cyber conflict in the Asia-Pacific Region. It then analyses the link between cyber capabilities and conventional military capabilities of the selected small states. Finally, the chapter investigates the contribution of cyber power to the foreign policy strategies of selection states.

Chapter 5 applies the second part of the framework by explicating the potency of strategic culture as a necessary *secondary* condition for the development of cyber capabilities. The chapter contends that strategic culture is a secondary condition because it registers the strategic preferences of small states and adapts foreign policy responses based on these preferences. This state level condition is analysed in three stages. The first examines the contribution of strategic culture in establishing the network readiness of selected small states. The second stage considers the role of strategic culture in development developing cyber strategies. The third traces the influence of strategic culture in designating government agencies responsible for managing cybersecurity issues.

Chapter 6 address the second corollary question in the study by clarifying the utility of cyber capabilities for small states. It argues that cyber capabilities are only useful for small states if they have a technology-oriented military force and if they are only employed for signalling foreign policy preferences. The chapter proceeds in three phases. First, it evaluates the conditions under which cyber capabilities can be advantageous for small states. Second, it probes the applicability of existing strategic concepts to the cyber operations by uncovering the adjunct function of cyber capabilities that supplements existing foreign policy instruments. Third, it compares the feasibility and usefulness of cyber operations in the context of the selected small states.

Chapter 7 reflects on implications of the study by considering the key theoretical and policy contributions of the study that make the prepositions and concepts valuable for both academic and policy communities. The chapter first explains the relevance of existing theoretical frameworks and concepts in explaining state interactions in cyberspace. It then discusses the validity of the much publicised cyber revolution thesis for the strategy of small states. The last part of chapter proposes vital research themes that remain unexplored in emerging area of study.

# Chapter 2
## Mind the Gap: The Literature on Cybersecurity and International Relations

Cyberspace as an environment for state interaction has generated profound implications for international security. On one hand, cyberspace has provided opportunities for states to cooperate more effectively in terms of intelligence collection and special operations. On the other hand, the prevalence of cyberspace has also given rise to unique threats requiring direct policy responses from decision-makers. While these interactions continue to influence state behaviour, there has been slow progress in studying these critical issues since it is unclear if existing theories and explanations are able to interpret cyber phenomena (Kello, 2013).

The literature on cyber studies has increased significantly in the past decade; however, scholarship on cyber conflict and related topics tends to be highly specific, policy-oriented, and does not necessarily contribute to the building or testing of theories central to the study of International Relations (Dunn Cavelty, 2013).

Within the literature that can be considered as academic, most studies have focused on powerful states, particularly the competition and conflict between China, the U.S. and Russia. Despite the participation of numerous states in cyber interactions, the relevance of small states in cyber conflicts has generally been neglected (Burton, 2013). The significance of this scholarship gap is even more prominent in the studies on the Asia-Pacific, where a substantial amount of literature has focused on the strategies of small states due to the enduring security dilemma in the region. Since the start of this century however, very few studies have examined the impact of cyber capabilities on the foreign and security policies of small states in the region.

Against this backdrop, this chapter evaluates three key themes within the literature on international relations and cyber studies with the objective of identifying the specific gap and defining the potential contributions to the literature. The first theme considers the political and security dynamics in the Asia-Pacific, particularly the responses of weaker states to great power rivalry and the arms build-up in the region. The second theme looks into small states in international relations with emphasis on the factors that shape their foreign policy and behaviour. The third theme focuses on cyber studies and international relations, specifically discussing the debates regarding the impact of the information revolution on states, cyberspace as a domain of conflict, the motivations for developing cyber capabilities, the cybersecurity of small states and finally, a survey of existing theoretical contributions to cyber studies.

## Geopolitics in the Asia-Pacific

*Responses to the great power rivalry*

Scholars and analysts have argued that the political and security instability in the Asia-Pacific will shape the dynamics of international relations in the twenty first century. The region has been characterized by major shifts in the balance of power, uneven distributions of economic and political power within and between countries, weak security institutionalization, and intense territorial disputes (Betts, 1994; Christensen, 1999). Compared to other great power dilemmas such as Russia's assertiveness or America's rebalancing strategy, China's rise to power has proven to be a more threatening situation because of its rapid military modernization (Shambaugh, 1996; Mearsheimer, 2010) and strong soft power projection in the region and beyond (Kurlantzick , 2007; Woods, 2008).

This regional instability has influenced weaker states to develop strategies for survival by cooperating with other states and enhancing their own military capabilities. To be certain, scholars have advanced several foreign policy strategies that capture the interaction between weak states and great powers in the context of the Asia-Pacific region. These strategies can be classified into three categories: accommodation, self-reliance and opposition. State behaviours within the strategy of accommodation are conceptualized as *bandwagoning* and *engagement*. *Bandwagoning* is defined as allying with the state that poses the principal threat (Waltz, 1979/2010), while *engagement* refers to strategic mode of actions in which the "building of interdependencies and dialogues are instrumental policies to change the behaviour of a target state" (Lynch, 2002, p. 187)

The strategy of self-reliance, meanwhile, is reflected in four types of behaviour: *leash slipping, neutrality, hedging,* and *transcending*. *Leash slipping* can be considered as a self-reliance strategy because it involves building-up or enhancing military capabilities to maximise the ability of states "to conduct an independent foreign policy" (Layne, 2006a, p. 9). *Neutrality* is considered a form of self-reliance because it intends to avoid any entanglement or conflict caused by great powers. The strategy is based on a "principled belief whose core consists of interests-based, normative ideas on foreign and security-policy orientation" (Goetschel, 1999, p. 117). *Hedging* is another form of self-reliance that focuses on maintaining an independent foreign policy. It is defined as "a set of strategies aimed at avoiding (or planning for contingencies in) a situation in which states cannot decide upon more straightforward alternatives such as balancing, bandwagoning, or neutrality" (Goh, 2006, p. 2). Lastly, the strategy of *transcending* involves engaging international institutions to avoid any entanglement with great powers. Paul Schroeder (1994, p. 117) defines *transcending* as "attempting to surmount international anarchy and go beyond the normal limits of conflictual politics through some institutional arrangement, international consensus or formal agreement on norms, rules and procedures…"

The strategies that aim to oppose great powers are composed of two types: *balancing* and *soft balancing*. *Balancing*, as defined by Walt (1985), involves allying with other states to oppose the principal source of threat. The traditional notion of *balancing* involves balancing internally through arms build-up and externally through alliances with other states. *Soft balancing* however, is a variation of balancing that involves the use of economic statecraft and non-military tools such as diplomacy to delay, frustrate, and constrain the actions of a hegemon (Pape, 2005).

Aside from these strategies, multilateral responses to the aggressive posturing of great powers have also been suggested. Haacke (2009, p. 427) for instance, argues for the increased role of the  Regional Forum (ARF) in addressing insecurity and disputes: "while the ARF primarily remains a forum for regional security dialogues and confidence-building, its participants have slowly become prepared to proceed with practical security co-operation..." Egberink and van de Putten (2010, p. 132) have also highlighted the importance of multilateral institutions in Asia: "There seems to be a consensus among observers that during the past two decades, Association of Southeast Asian Nations (ASEAN) has led to stable relations between the great powers in Asia. It is thought to have mainly done so by establishing new channels and platforms for communication."

Despite the substantial literature on strategies to manage great powers, few studies have examined how information technology can affect the foreign policy strategies of small states in the region. This neglect is mainly due to the lack of access to relevant data for producing academic studies as well as the insufficient number cyber conflict cases, that can be observed (Liff, 2012). This study aims to address this gap by assessing if the geopolitical conditions have any relevance on the development of cyber capabilities as well as by understanding how these capabilities can potentially contribute to foreign policy strategies identified in the literature. This contribution is important because it advances extant knowledge about small state behaviour, and explains the relevance of cyber capabilities as a foreign policy instrument of states.

### *Arms build-up in the region*

Another key issue in the literature is the debate on the arms build-up in the region. One view is that China's rapid military modernization has influenced other states to increase defence spending and modernise their military forces (Roy, 1994; Hughes, 2009). Another interpretation by Bitzinger (2010, p. 65) contends that the arms build-up in Southeast Asia is part of an arms dynamic but not necessarily caused by China's rise: "weapons acquisition under the arms dynamic, therefore, while resembling an arms race in many ways, is actually a "non-cataclysmic" process of arms acquisition intended to preserve "status-quo" oriented rivalries…" Moreover, other scholars have emphasized alternative causes for the arms build-up: inter-state tension, internal security, domestic politics, geopolitics, strategic cultural conditions and prestige (Ball , 1994; Tan , 1997; Collins , 2003; Loo , 2005; Hartfiel and Job, 2007).

While the arms build-up in Asia has constantly been studied since the end of the Cold War, few scholars have examined the impact of the development of cyber capabilities as a part of the arms build-up. Hartfiel and Job (2007) and Bitzinger (2010) for instance, point out the significance of the acquisition of advanced military technologies by different states, but do not include cyber capabilities in their analysis. This absence of cyber studies on the Asia-Pacific can be attributed to two factors: the limited access to data required for academic studies and the general scholarship gap in the subject of cyber studies (Reardon and Choucri, 2012).

In reviewing extant studies, it is apparent that most have focused on China. As Ball (2011, p. 81) asserts, it has "the most extensive and most practised cyber-warfare capabilities in Asia." While there have been some notable contributions to the cybersecurity literature on the region, such as by Thomas (2009) Ortis and Evans (2011), and Chong (2014), these studies are still very limited compared to works on conventional military capabilities. In this regard, this study intends to address this gap by assessing the significance of cyber capabilities in relation to conventional military capabilities for small states. This assessment is necessary given the limited academic studies on cybersecurity and more notably the proliferation of cyber capabilities in the Asia-Pacific region.

## Small States in International Relations

*Sources of foreign policy*

Debates regarding the sources that influence small state foreign policy have generated different views within this body of literature. Previous studies suggest three general sources that shape foreign policy: systemic, state and individual. Systemic sources focus on relative power distribution between powerful states as the main source of foreign policy formation (Waltz 1979/2010). Since small states have limited resources and military capabilities, their foreign policies are usually reactive and significantly influenced by the prevailing distribution of power. This observation is supported by Cammack (1988 ), Handel (1991) and Nye (2007), who contend that the power distribution in the international system outweighs other explanatory variables in influencing the foreign policy of small states.

On the other hand, other studies contend that state-level sources, such as the societal groups and national characteristics, have the most influence on the formation and change of small state foreign policy. For instance, Doeser (2011) observes that domestic sources facilitated change in the Danish "footnote policy" during the mid-1980s. He points out that political party opposition and public opposition created "opportunities for the government to use foreign policy change as a strategy to increase its political power on the domestic scene" (Doeser, 2011, pp. 223-224). Moreover, Kibbe's (2012) study on Cuba also recognizes the significance of state-level sources of foreign policy. She argues that rather than Soviet influence, it was deeply ingrained internationalist ideology and cultural roots that shaped Cuba's decision to dispatch troops to Angola from 1975-1976.

A third source that can shape the formation of small state foreign policy is the role of individuals. An example of individual influence on foreign policy, is Williams' (2012) work on Romania's resistance against the Soviet Union. Williams (2012) argues that the refusal to send troops to invade Czechoslovakia in 1968 was mainly motivated by Nicolae Ceausescu's interest in gaining more power and control in Romania. She maintains that Ceausescu was depending on Romanian nationalism to legitimise his decision to pursue an independent foreign policy and challenge the Soviet Union's policy vis-à-vis Czechoslovakia (Williams, 2012). Another example is the primacy of elite ideas and preferences over other foreign policy sources. A recent study by Gvalia et al. (2013) argues that Georgia's balancing behavior against Russia can be better explained by examining individual level sources specifically elite ideas and preferences rather than changes in its external security environment. The scholars' consultation with political elites and experts revealed that despite the Russia-Georgia War in 2008, Georgia's political elites were not persuaded "to alter its Western-oriented foreign policy to accommodate Russian interests" (Gvalia et al., 2013, p. 110).

Due to the complexity of foreign policy decisions, scholars such as Beasley, et al. (2002), Hudson (2006), Breuning (2007), and Carlsnaes (2016) suggest that multifactor explanations are more appropriate in generating rich and comprehensive explanations compared to single explanations. For example, influential works by Putnam (1988) and Evans (1993) reveal the significance of the interplay between domestic and international sources in shaping foreign policy behavior. Moreover, studies by Hey (2003) and Larsen (2005) confirm that multiple sources can provide more convincing explanations regarding the foreign policy behaviour of small states. This study therefore, builds on previous literature by advancing a multifactor explanation for the formation of foreign policy. More specifically, it draws on systemic (main cause) and state sources (intervening cause) to explain the development of cyber capabilities in small states. It makes a contribution to this body literature by using foreign policy analysis to explain the strategic utility as well as the limitations of cyber capabilities for the small states.

*Foreign policy behaviour*

Another core issue in studying small states is explaining foreign policy behaviour. The most comprehensive list of behavioural tendencies to date has been compiled by Hey (2003). Her work enumerates a number of observed behaviours that capture a substantial amount of work on small states, particularly their inclinations towards: (i) engaging in low level of participation in world affairs; (ii) addressing a narrow scope of foreign policy issues; (iii) limiting their behaviour to their immediate geographic area; (iv) employing diplomatic and economic foreign policy instruments as opposed to military instruments; (v) emphasising international norms and laws; (vi) working with multinational institutions; (vii) choosing neutral positions; (viii) depending on superpowers for protection, partnership, and resources; (ix) cooperating and avoiding conflict with others; and (x) spending a disproportionate amount of resources on ensuring physical and political security and survival. These tendencies are often mentioned by scholars studying small states in sensitive geopolitical regions, such as the Eastern Europe (Mehdiyeva, 2011; Shlapentokh, 2012; Gvalia et al. 2013), Southeast Asia (Goh, 2007; Cheng –Chwee, 2008) and South America (Resende-Santos, 2007; Williams et al., 2012).

The list however, is not complete since it lacks some important behavioural tendencies articulated by other scholars such as Barston (1973) and Keohane (1969). Barston (1973) emphasizes that the weakness of a small state can be a source of bargaining power through the strategic significance of its territory, and Keohane (1969) points out that a small state can develop political leverage by deepening its political capital with great powers. Conversely, Inbar and Sheffer (1997) observe that changes in the distribution of power in the international system have affected the capabilities of small states, allowing greater freedom of action for regional actors to pursue their particular interests.

The study contributes to this body of literature by challenging at least two observed behaviours posited by scholars. First, the study challenges the observation that small states exhibit a low level of participation in international affairs. Studies by Nye (2010), Manjikian (2010), (Sheldon, 2011), and Betz (2012) suggest that cyber power may enhance the political influence and international standing of small states, thereby providing more options for their respective foreign and security policies. Building on these findings, the study investigates how highly networked small states in the Asia-Pacific make use of cyber capabilities as a tools to defend their national security interests and maintain their relevance in international affairs. Second, it contests the observation that small states choose neutral positions in international relations. The study aims to refute this observation by proving that some small states in the Asia-Pacific use advanced technology and employ resilient strategies to engage with more powerful states.

In terms of policy, this study contributes to the military strategy and foreign of small states by clarifying the utility of cyber capabilities. Since "strategic thought on cyber conflict is still in its infancy", this study can serve as an assessment of the utility of cyber capabilities for small states (Sloan, 2012, p. 85), This study will be relevant for defence planners and policy-makers given the lack of academic research and policy assessments regarding the strategies of less powerful states in cyberspace. If cyberspace is not a decisive warfighting domain, then what strategic purpose can it achieve for small states?

## Cyber Studies and International Relations

### *Impact of the information revolution on states*

The impact of the information revolution on relations between states is arguably the most prominent issue in this body of literature. The literature is generally influenced by two dominant arguments: *cyber-optimism* and *cyber-scepticism*. The cyber-optimists, which include Joseph Nye, Robert Keohane and Nazli Choucri, contend that the information revolution has continued to change the way states interact. More specifically, Keohane and Nye (1998) suggest that the information revolution has dramatically transformed one aspect of interdependence between different actors in the international system. They assert that the networks created through the information revolution have vastly increased the number of channels of communication between societies. Choucri (2012, p. 233) asserts that cyberspace has created new challenges for different actors in the international system: "Given the rapid growth of Internet users, the increased complexity of managing cyberspace, and the record of governments' control or denial of access, it is reasonable to consider the potential trajectories of international relations and their cyberpolitics." Nye's (2010, p. 1) contribution has also stressed the significance of changes in power relations due to cyberspace: "The characteristics of cyberspace reduce some of the power differentials among actors, and thus provide a good example of the diffusion of power that typifies global politics in this century."

In contrast, cyber-sceptics view the information revolution, particularly digital new media in a more cynical light since it provides states with innovative tools for the delivery of state propaganda, surveillance and censorship. For instance, Morozov (2012) challenges the widely held perception of the Internet as a tool for promoting democracy by explaining how social media platforms like Facebook and Twitter enable states such as Russia and Iran to crackdown on ordinary citizens and entrench their own dictatorships. On the other hand, McChesney (2014) also argues against the positive effects of the Internet, not because of its unique qualities, but mainly because capitalism in the form of powerful private companies has exploited and dominated the Internet thereby undermining and weakening democratic practices online.

The study builds on the sceptical view on the debate on information revolution. Drawing on previous studies, the study proceeds with the premise that while information technology can facilitate the advancement of foreign policy, computers and networks do not change how states interact. This premise is based on existing studies that challenge the revolutionary impact of information technology on strategic affairs (Betz and Stevens, 2011; Rid, 2012, Gray 2013). Following this view, the study's contribution is to specify based on empirical data, how small states can make utilise information technology to advance their respective foreign policy interests.

### *Cyberspace as a domain for conflict*

There are generally three distinct views or schools of thought that have influenced the debate on cyber war: "revolutionists", "traditionalists", and "environmentalists" (Langø, 2013). Revolutionlists led by John Arquilla and David Ronfelt (1993), maintain that cyber warfare is an emerging mode of conflict that persists and continues to develop. These scholars argued that the information revolution would change the dynamics of war: "Warfare is no longer primarily a function of who puts the most capital, labor, and technology on the battlefield, but of who has the best information about the battlefield" (Arquilla and Ronfelt, 1993, 141). Dorothy Denning (1999, p. 67) contends that while future war cannot be predicted, "information warfare, in all its manifestations -

espionage, intelligence operations to electronic warfare to psychological operations and perception management" - will play an important role. Gregory Rattray (2001, p. 20), takes a similar position, asserting that "the use of non-violent digital attacks to achieve political objectives must be understood as part of a new form of warfare." Andrew Krepinevich (2012) meanwhile, highlights the revolutionary potential of cyberspace: "…the potential exists for a cyber attack to inflict relatively prompt, catastrophic levels of destruction on the United States and other developed world states with advanced infrastructures—*provided one accepts a broad definition of what constitutes "catastrophic" destruction.*" Finally, Stone (2013, p. 107) asserts: "cyber war is possible in the sense that cyber attacks could constitute acts of war. This point only becomes evident, however, if we are clear about what is encompassed by the terms 'force' and 'violence', and about their relationship with the matter of lethality."

In contrast, traditionalists are sceptical "about the effects of the information revolution on international security and relations" (Langø, 2013, 19). Martin Libicki (2007, p. 3), one of the main proponents of this view, cautions that "hostile conquest" in cyberspace "may be less consequential than meets the eye" due to the inherent limitations of cyber warfare. Betz and Stevens (2011, p. 95) argue that the concept of "Cyber war as a "pure play" or "single focus" option for states is unrealistic because of the expanse and range of their interests and capabilities." Eric Gartzke (2013, p, 72) is likewise doubtful about the potential of cyberspace for war: "Students of cyberwar have yet to explain how the internet can host meaningful political conflict precisely because it cannot serve the final arbiter function that has for millennia been the purview of physical violence." Brandon Valeriano and Ryan Maness (2014, p. 359) confirmed through quantitative analysis that "cyber disputes are rare" and "when they do happen, the impact tends to be minimal." More recently, Patrick Porter (2015, p. 204) asserts that cyber may not be a "game-changer" for international politics. He submits: "contrary to apocalyptic visions of cyber capabilities, the cyber domain is difficult to launch crippling attacks within."

The environmentalist school of thought offers a third perspective in the study of cybersecurity. This school does not directly engage in the debate on cyber war but is included in this section because of its focus on power in the context of cyberspace. This approach is argued to be more inclusive because studies that follow this view "seek to define and measure the inherent characteristics or features of cyberspace as a distinct environment, separate from other domains and greater than the sum of its technological parts" (Langø, 2013, 27). Joseph Nye (2010, 2011) is a prominent scholar in this school of thought because of his influential work on cyber power. Nye's (2011, 123) conception of cyber power is comprehensive: "Cyberpower can be used to produce preferred outcomes *within* cyberspace, or it can use cyber instruments to produce preferred outcomes in other domains *outside* cyberspace." Another interpretation of cyber power is presented by Kuehl (2009, 38): "While cyberspace as an environment simply "is", cyberpower is always a measure of the ability to use that environment. Technology is one obvious factor, because the ability to "enter" cyberspace is what makes it possible to use it." John Sheldon (2013, 310-311) contributes to this view by offering three key the attributes cyber power: pervasive (able to generate strategic effects in other domains), complementary (enables other instruments of states) and stealthy (difficult to detect and attribute cyber intrusions).

In terms of the cyber warfare, traditionalists have questioned the validity of the concept. Libicki (2012, p. 322) postulates that it is misleading to consider cyberspace as a war-fighting domain since it is "not helpful when it comes to understanding what can and should be done to defend and attack networked systems." Thomas Rid (2013, p. 4) meanwhile, contends that the concept of cyber warfare is flawed because military actions in cyberspace cannot satisfy Clausewitz's perennial definition of war: "violent, instrumental in character and politically attributed." In addition, he argues that all reported cases of cyber intrusions can be considered as forms of conventional strategic instruments already employed by states: espionage, sabotage and subversion (Rid, 2013).

Phillip Meilinger (2010) offers a strong challenge to the traditionalist view that is sceptical of cyber warfare. He asserts that historians and generals are mistaken in "equating land warfare—specifically, conventional battle as once practiced—with war" because this "reflects institutional bias and downplays the role of technology" (p. 26). More specifically he points out that:

"The nature of war is mutable. Warfare in the modern world remains deadly and destructive, but it need not be violent or bloody. The fundamental aspect of war in centuries past may have taken the form of sanguinary battles between infantrymen, but that is no longer necessarily the case" (Meilinger, 2010, p, 28). This study is largely informed by a traditionalist view in exploring how cyber capabilities impact the strategies of small states. This view is adopted by the study because it is grounded on empirical realities that appropriately capture state interactions in cyberspace. Revolutionists tend to exaggerate the impact of network-technology on strategic affairs while environmentalists cannot sufficiently account for conflict and aggression in cyberspace. Indeed, while there have been confirmed cases of state aggression in cyberspace, the study is not concerned with the occurrence of interstate conflict in cyberspace, rather it focuses on understanding why small states have developed cyber capabilities as well as the utility of these capabilities. In this regard, the study's contribution is to build on the limitations of cyber capabilities as articulated by prevailing literature, and develop an alternative explanation to address the puzzle of the study using a specific theoretical lens.

*Motivations for developing cyber capabilities*[5]

Another key issue within the literature on cyber studies is the purpose and utility of cyber capabilities. Most studies on the subject analyse the implications of cyber conflict on state interaction without addressing the fundamental question of why states develop cyber capabilities in the first place. The literature on international relations provides four potential answers to this question: to defend against attacks, to enable conventional capabilities, to exploit a new environment and to compete for military dominance.

Policy-makers and some academics argue that cyber capabilities are necessary for defence against increasing and sophisticated cyber attacks from unknown actors. William Lynn (2010) contends that warfare in cyberspace is a substantial and imminent threat because a range of different actors have access to the hardware and knowledge to execute cyber attacks against states. He advocates that the unique characteristics of cyberspace require a vigorous defensive capability by employing the following distinct measures:

> "treating cyberspace as an operational domain, like land, air, sea, and outer space; employing active defences to stop malicious code before it affects our networks; protecting commercial networks that operate the critical infrastructure that our military relies upon; joining with allies to

[5] This section is adopted from Domingo (2014a)

> mount a collective cyber defence; and mobilizing industry to redesign network technology with security in mind" (William Lynn, 2011,).

James Adams offers a similar perspective, arguing that the US is vulnerable to attack particularly because of the smaller nations and private groups that would seek to gain an advantage by employing asymmetric warfare. He explains that US military has become increasingly dependent on new technology, to the point that it is paradoxically making itself more vulnerable to escalating incidences of complicated cyber attacks. Adams asserts that an effective defence and coherent strategy to counter the cyber-threats to national security will only be feasible with the cooperation of the private sector (Adams, 2001). Richard Clark and Robert Knake (2010, p. 32) maintain: "there is every reason to believe that most future kinetic wars will be accompanied by cyber war, and that other cyber wars will be conducted as "stand-alone" activities, without explosions, infantry, airpower, and navies." Martin Rudner (2013), on the other hand, focuses his analysis on cyber attacks that are specifically directed at critical national infrastructure. Critical infrastructures, he observes, are more susceptible to cyber attacks from a wide spectrum of perpetrators because of their high value and fundamental vulnerabilities, in addition to the significant potential to inflict extensive destruction on targeted states. Rudner (2013, p. 473) argues that "a proactive, intelligence approach to cyber-security" is a vital defensive strategy because intelligence can improve the ability of governments to assess the effects of cyber attacks, mitigate the risks, and streamline cyber-security into an efficient process based on informed decisions.

A second potential answer is that states develop capabilities in cyberspace because they are useful enablers of conventional military operations. Martin Libicki (2009) argues that during the absence of physical military operations, computer network operations cannot lead to the occupation of territory. He explains however, that offensive cyber capabilities are worth developing "because a devastating cyber attack may facilitate or amplify physical operations and because an operational cyber war capability is relatively inexpensive" (Libicki 2009, p. 144). Furthermore, Libicki (2007) suggests that military cooperation in cyberspace may be more advantageous for states:

> "The possibilities of hostile conquest in cyberspace may be less consequential than meets the eye while the possibilities of friendly

> conquests ought to be better appreciated. The current obsession with hostile conquest fosters a tilt towards  closed systems and at least among states who have powerful systems to begin with" (p. 3).

Colin Gray (2013, p. 44) supports Libicki's view, emphasizing that military operations in cyberspace can only be an enabler of physical effort because "stand-alone cyber action is inherently grossly limited by its immateriality." He contests that while independent cyber action certainly is possible, "the strategic logic of such behaviour, keyed to anticipated success in tactical achievement, is not promising" (Gray, 2013, p. 44) . Finally, he concludes that the most probable use for cyber capabilities in cyberspace would be "a contributing enabler of effectiveness of physical efforts in the other four geographies of conflict."

Betz and Stevens (2011, p. 96) share an analogous interpretation: "Military cyber-power is a real and important complement to other military capabilities. It does not, as airpower did not, obviate those capabilities or change." Moreover they contend that while military cyber power complements other military capabilities, the concept of "cyber war" as a "strategically decisive form of interstate warfare is a confusing and pointless distraction" (Betz & Stevens, 2011, p. 96).

The new environment is a third potential explanation, and it posits that states develop military cyber capabilities to take advantage of the lack of control and regulation in cyberspace. Scholars who support this explanation have identified two critical issues regarding the new environment: the attribution problem and the lack of a treaty for cyberspace. Since multiple hostile actors operate in cyberspace, attribution or identifying the agent responsible for attacks is a critical concern for national-states because it affects their ability to deter potential attacks. David Clark and Susan Landau (2011, p. 28)  however, stress that the "solutions to the "attribution problem" lie outside the technical realm, and are instead in the space of law, regulation, multi-national negotiation, and economics." Hence, Clark and Landau's analysis implies that the use of advanced military technology without a political direction is insufficient to address hostile action in cyberspace.

Another major concern is formulating an international treaty to define acceptable activities in cyberspace. The strategic utility of cyberspace remains unclear, but since states have recognized it as a "domain of warfare", they are now in the process of creating credible military capabilities for waging offensive war in cyberspace. While there is no guarantee that a treaty will prevent conflict, Rex Hughes (2010) points out that the absence of meaningful regulation or treaty infrastructure in cyberspace may escalate existing conflicts and increase the potential of an interstate war. Given that states already have cyber capabilities, according to Hughes the way forward is for international society led by China, Russia, India, Japan and the U.S., to initiate the creation of a treaty for cyberspace.

The competition for military dominance is a fourth potential explanation as to why states develop cyber capabilities in cyberspace. The central theme of this explanation is based on the logic of realism: in an anarchic system, states are mainly concerned with the intentions and capabilities of their competitors. Since there is no definitive way of predicting the behaviour of competitors, states are forced to develop more effective and advanced military capabilities. Kenneth Waltz (1979/2010, p. 105), the most prominent proponent of this view, suggests that competition between states induces military innovation: "Contending states imitate the military innovations contrived by the country of greatest capability and ingenuity. And so weapons of major contenders, and even their strategies, begin to look much the same all over the world."

John Mearsheimer (2001) shares the same view but adds that the best way for any state to guarantee its survival is to be much more powerful than its other competitors, because weaker states are unlikely to attack it for fear they will be defeated. In competing for power, he points out that "states do not develop new technologies simultaneously", which means that in the case of cyber capabilities, the innovator often gains significant, but temporary, advantages over the laggard (Mearshiermer, 2001, p. 231). Emily Goldman (2007) on the other hand, explains that tension between states creates strong incentives to improve military responsiveness, leading to increased military expenditures, acceleration of research, development, and experimentation. By investigating the development of American and British Naval Air Power from 1919 to 1945, Goldman (2007) confirmed that there is indeed a relationship between international competition and military effectiveness.

Another variation of this explanation is what João Resende-Santos (2007) describes as military emulation. Military emulation according to Resende-Santos

(2007, p.2) is "the deliberate systematic imitation of the military technology, organization, and doctrine of one country by another." It is the result of states' concern with relative competitive effectiveness, or their overall capacity to meet the changing requirements of sustainability and success in the international system. In this regard, the development of cyber capabilities is a manifestation of military emulation since states would be using parallel expertise and the technology required for executing sophisticated computer network operations (Billo and Chang, 2004).

The study contributes to the debates regarding cyber capabilities by testing the validity and representatives of these explanations in the context of selected small states. Since a number of existing studies support the "defensive" and "enabler" explanations for developing cyber capabilities, (Chong, 2012; Dunn Cavelty, 2013; Gamreklidze, 2014) this study can challenge or affirm these explanations by offering more compelling justifications and providing more insights about the motivations of small states using a different theoretical lens. Engaging with existing theories to explore the cyber phenomena is necessary because theories provide systematic explanatory frameworks that integrate valid concepts and develop modest generalisations regarding the development of cyber capabilities. Moreover, given the underdeveloped literature on cyber strategy of small states, the study also contributes to existing knowledge by locating the experience of small states within wider literature on cybersecurity and international relations.

### *Cybersecurity and small states*

The literature on cyber studies has mostly focused on analysing the actions of great and rising powers because of their potential impact and influence on state interaction in cyberspace (Ebert and Maurer 2013). However, the proliferation of cyber capabilities has influenced scholars to refocus their attention on small states, therefore slowly addressing the substantial scholarship gap in cyber studies. An important issue that has been discussed is the response of small states towards increasing and sophisticated cyber attacks. Focusing on Estonia, Matthew Crandall (2014, p. 49) underscores that small states need to exhaust both domestic and international resources to address cyber threats: "Estonia has mostly used international organizations to address its cyber-security issues… Despite the success Estonia has had in its international efforts, it has still made cyber-defence a priority on the national level as well." On the other hand, Gorazd Praprotnik et al. (2012, pp. 274-275) examine the developing nature of Slovenia's cyber capabilities: "Slovenia is not adequately prepared for cyber-attacks, especially for advanced attacks on its critical information and communication infrastructure." They recommend that the government should improve coordination between civilian agencies, military forces and the private sector to effectively address cyber attacks.

Alan Chong (2012, pp. 246-247) explains the complexities of Singapore's experience with cyber issues: "Singapore's encounter with information warfare is riddled with layers of ambiguity. It is certainly not a case of straightforward offence and defence across demarcated boundaries." Furthermore, he points out that the civilian sector deals with cyber offense and defence while the SAF utilises cyber capabilities to enable conventional military capabilities. In the context of New Zealand, Joe Burton (2013, p. 216) maintains that "a globalised cybersecurity environment is eroding New Zealand's geographical isolation." He contends that New Zealand is facing various domestic and international challenges in addressing cybersecurity, the most prominent of which is the struggle to balance security and privacy in response to cybersecurity issues.

A second issue that is central to this debate is the idea that small states can derive asymmetric advantages in cyberspace. The logic of asymmetric advantage postulates that barriers to entry for small states are decreasing while the vulnerabilities of powerful states are increasing (Knapp and Boulton, 2006). Ross Rustici (2011, p. 36) explains the strategic advantages of cyberspace for small states: "Cyber capabilities allow, for the first time in history, small states with minimal defence budgets to inflict serious harm on a vastly stronger foe at extreme ranges." Drawing on parallels between nuclear and cyber weapons, Joseph Nye (2011, p. 23) explains the advantages for small states: "the belief that new weapons are "equalizers" that allow smaller actors to compete directly but asymmetrically with a larger state." Similarly, Liina Areng (2014, p. 11) emphasizes: "Digital power gives a clear asymmetric advantage in national security to small states." She claims that while powerful states invest substantially in the development of cyber capabilities, small states still have more opportunities to compete in this domain because, "mass" is no longer a decisive factor in cyberspace (Areng, 2014, p. 6).

On the contrary, several scholars have contested the idea of asymmetric advantage for small states. Using the Stuxnet as an example, Jon Lindsay (2013) showed that cyber capabilities are not necessarily a "weapon for the weak" since small states are confronted by steep barriers to weaponization for inflicting meaningful damage. He concludes therefore that the asymmetric advantage proposed by cyber optimists is misleading because the evidence of cyber conflict suggests a reverse view: cyber capabilities favour powerful states. Eric Gartzke (2013) demystifies the idea of asymmetric advantage, asserting that cyber capabilities cannot deter or compel other states effectively because cyber attacks are not as consequential as kinetic attacks. In this sense, he maintains "Cyberwarfare will most often occur as an adjunct to conventional warfare, or as a stop-gap and largely symbolic effort to express dissatisfaction with a foreign opponent" (Gartzke, 2013, p. 73). Moreover, a recent study by Alison Russell (2014, p. 145) that examined Estonia and Georgia, argues that geographically small states are more vulnerable to what she refers to as a "cyber blockade"[6], since they have fewer external networks and potentially less resilient cybersecurity systems.

This study makes two distinctive contributions to the literature on cybersecurity and small states. First, the study advances the comprehensive literature on small states foreign policy by assessing the utility of cyber capabilities as an instrument for managing foreign policy dilemmas. This is important because the existing literature on small states is predominantly focuses on traditional foreign policy strategies such as diplomacy and does not account for the impact of network-technology in foreign policy behaviour. Second, the study follows the traditionalist interpretation of the cyber revolution and tests the logic of asymmetric advantage on selected states in the Asia-Pacific. Verifying the perceived asymmetric advantage offered by cyberspace is necessary because it rectifies a strong misperception regarding the cyber revolution and more importantly, it clarifies what cyber capabilities can really contribute to the strategic predicament of small states

*Theoretical contributions*

[6] Cyber blockade is defined as "an attack on cyber infrastructure or systems that prevents states from accessing cyberspace, thus preventing transmission of data beyond geographical boundary" (Russell, 2014, p. 7).

Another issue that has been critical to cyber studies is the sparse contribution of existing studies to International Relations theory. There is no clear debate on this issue but scholars have underscored the theoretical gap in the literature on cybersecurity. Miriam Dunn Cavelty (2007, p. 20) for example, claims that the difficulties of studying the impact of the information age on international relations are considerable "because previous work on the subject is relatively sparse, disorganized, and hardly informed by International Relations theory or other theoretical approaches." Adam Liff (2012, p. 403) echoes the same view: "Despite its increasing salience to policymakers and defence planners, the issue of cyber warfare has not caught the attention of most students of international relations. Much of the limited literature has emerged from US war colleges, policy-oriented research institutions, and think tanks and is often under-theorized." More recently, Madeline Carr (2017, p. 2) offers a similar observation: "Most of the existing work on this emerges from scholars working on military doctrine or strategic studies with a particular (and somewhat repetitive) emphasis on the writings of Clausewitz."

There are a few scholars that contributed theoretically informed studies early in the study of cybersecurity. A prominent example is the work on securitization theory and cybersecurity. Bendrath (2001), Dunn Cavelty (2008), Hansen and Nissenbaum (2009), and Lawson (2011) have used this theoretical framework to explain how different actors in international relations have securitised the perceptions of states towards the cyberspace, thereby exaggerating policy responses to cyber threats. Another exception is Eriksson and Giacomello (2006) who argued for the relevance of theoretical approaches in studying cybersecurity. They maintained that "the liberal focus on pluralism, interdependence, and globalization, the constructivist emphasis on language, symbols, and images (including "virtuality"), and some elements of realist strategic studies (on information warfare) contribute to an understanding of digital-age security" (Eriksson and Giacomello 2006, p. 221).

Geoffrey Herrera's (2006, p. 2) work that examines the "relationship between technological change and international system change", is another early contribution that is draws on historical sociology and constructivism to track the evolution of sociotechnical systems. The study reveals that technology and international politics are mutually constitutive: "Technology is part of the structure of international politics; international politics is one of the factors governing technological change."

More recent studies have been more theoretically engaged in exploring the intersection between power, technology, and relations between states. One example of such study is McCarthy's (2015, p. 4) work, in which he offers a "theoretical reconsideration of the relationship, in IR theory, between power and technology." He contends "that technological artefacts must be considered as institutions with specific cultural norms and values embedded within their physical makeup." Another example is Valeriano and Maness' (2015) pioneering empirical study that draws on their unique Dyadic Cyber Incident and Dispute Dataset to characterise and explain the cyber conflict in the international system. The study asserts that cyber interactions between states are characterised by restraint and regionalism, challenging the hype and threat inflation surrounding cybersecurity issues.

A third example is Carr's (2016, p. 77) innovative work that explores how digital technologies and the Internet have led to a power paradox: "states which have most successfully adopted and exploited the opportunities afforded by the Internet are also most vulnerable to the range of threats which accompany it." Since no single theory of power was suitable, a theoretical framework, that integrates insights from the philosophy of technology and the social construction of technology, was developed to explore the "conceptions of US power have influenced the development of the Internet and what implications this has for understanding power in the information age" (Carr, 2016, p. 16). A fourth example by Kello (2017, p. 12), offers a theoretical framework that clarifies the "two states of nature" in cyber politics: states locked in a traditional system of security competition, and a chaotic "global milieu" of non-state actors that are motivated towards subverting national or international order. The study illustrates how the widespread diffusion of the "virtual weapon" enables the convergence and collision of states and non-state actors, ultimately affecting the international order (Kello, 2017, pp. 12-13).

The emergence of theoretically informed works suggests two key ideas for academics studying the intersection of technology and international relations. First, it is necessary to thoroughly assess the explanatory power of existing International Relations theories before dismissing them as outdated and inappropriate. The authors discussed in the preceding section systematically evaluated existing theoretical frameworks before concluding that these theories were not useful in achieving their respective research objectives. Second, while theories are generally useful frameworks in understanding international relations, the rationale behind the application of particualrly theories must be clearly articulated. For instance, several authors discussed in the previous section argued for the significance of more theoretically informed works because of the predominance of policy-oriented works in cybersecurity (Dunn Cavelty, 2010, pp. 124-125; Liff, 2012). While these works are equally important, they do not designed to build generalisations and develop concepts that are necessary for advancing existing knowledge about cyber phenomena.

This study responds to the theoretical gap in cyber studies by using International Relations theory to explain the foreign policy preferences of small states. More specifically, the study draws on James Rosenau's (1980) comparative foreign policy framework to determine which levels of analysis is necessary to explain the development of cyber capabilities as a foreign policy instrument. Rosenau (1980) suggested that various explanatory factors are needed to account for foreign policy behaviour and he organized these factors according to five levels of analysis: system (international system), role (bureaucratic actors), government (relationship between government actors), society (public opinion and national culture), and idiosyncratic (individual).

Building on Rosenau's (1980) work, this study analyses the sources of foreign policy at the system and state levels to develop a more inclusive understanding of why small states develop cyber capabilities. The study draws on neoclassical realism as the theoretical framework because it can appropriately bridge two levels of analysis by combining system and state level factors into a single integrated framework (for more details see chapter 3). Neoclassical realism has been an instrumental theoretical framework for explaining state behaviour at a systemic level, while accounting for domestic intervening variables (Rose , 1998; Lobell, et al. 2009). Strategic culture, on the other hand, has been used as an intervening variable to supplement theories focused on national interests and the distribution of power (Lantis and Howlett, 2013). Therefore, integrating both theories into a framework has proven to be useful in explaining strategic behaviour of states (Schweller, 2003; Dueck 2005; Glenn 2009). Furthermore, although this system-state explanation has been used in previous work, very few of these studies focused on the intersection between small states and cyber studies, making the study's contribution more significant to the literature on international relations.

## Conclusion

In evaluating the various debates, this chapter uncovered important research gaps that impede deeper understanding of the complexities of state interactions in cyberspace. Based on the literature, it is clear that few studies have examined the cyber strategy of small states in the Asia-Pacific. On the other hand, scholars working on small states have been reluctant to make sense of cybersecurity issues in the region because of the lack of accessible data necessary for academic research. Recent studies however, have demonstrated that these challenges can be surpassed through more systematic and empirically grounded works on cybersecurity and international relations (e.g. Valeriano and Maness, 2015; Lindsay, et al., 2015; Slayton, 2017)

Following the link between geopolitics and cyber conflict, the study aims to makes two contributions to the literature on geopolitics and conflict in the Asia-Pacific. Firstly, it evaluates the connection between regional instability and the development of cyber capabilities, as well as determining how cyber capabilities can potentially contribute to one or more strategies identified in the literature. Subsequently, it also assesses the strategic utility of cyber capabilities for small states in the region, in the context of conventional military capabilities.

In terms of the literature on small states, the study aims to make three contributions to the literature by challenging at least three observed behaviours posited by scholars. It first challenges the observation that small states exhibit a low level of participation in international affairs by investigating how small states make use of cyberspace as tool for advancing foreign policy. It then challenges the observation that small states limit their behaviour to their immediate geographic area by examining how small states expand their interaction with the international community through cyberspace. Lastly, the study contests the observation that small states choose neutral positions in international relations by demonstrating that some small states can use advance technology to advance their respective interests.

The study aims to make four main contributions in the literature on cyber studies and international relations. Firstly, it specifies how small states can make use of the perceived advantages afforded by the information revolution on states. Secondly, it develops an alternative framework to explain the development of cyber capabilities by combining neoclassical realism and strategic culture into an integrated theoretical framework. Thirdly, it builds on the observed foreign policy behaviours of small states and evaluates the functionality of cyber capabilities as a tool for advancing foreign policy interests. Lastly, it follows the traditionalist interpretation of the cyber revolution, and tests the logic of asymmetric advantage on selected small states in the Asia-Pacific region.

In terms of strategy, the study intends to make two contributions to the foreign and security policy of small states. The first is since strategic thought on cyber conflict is still in its infancy (Sloan, 2012, p. 85), the study can serve as an assessment of the utility of cyber capabilities as a foreign policy tool for small states. The second contribution is that the study also distinguishes the cyber hype (perceived utility of cyber capabilities) from cyber reality (actual utility of cyber capabilities) in the context of small states.

The next chapter focuses on addressing a key research gap: the lack of theoretically informed studies in cybersecurity. The deficiency in the application of theory precludes the development of modest generalisations and analytical precision that are instrumental for meaningful analysis of cyber phenomena. In this context, the next chapter explores the significance of theory in making sense of cyber interactions and presents the theoretical framework that will guide the rest of the inquiry.

# Chapter 3
## Explaining Cyber Capability Development

Cybersecurity issues have increasingly been a concern for states but the range of plausible cyber conflict scenarios remains poorly understood by academics and policymakers. It is unclear how traditional security mechanisms such as deterrence, collective security, and coercive diplomacy apply to cyberspace (Kello, 2013, p. 7). If states intend to mitigate cyber conflicts and maintain stability, a better understanding of the mechanisms and conditions that influence cyber interactions is necessary. In this sense, theories are essential tools because they provide systematic frameworks for investigating cyber phenomena (Valeriano and Maness, 2015, p. 45). More specifically, theoretical frameworks are crucial for maximizing explanatory power, maintaining logical consistency, and developing generalizations based on specific conditions (Mearsheimer and Walt, 2013). The use of theory however, has not been a common practice in the study of cyber conflict and security.

Most of the discourse on cybersecurity is currently policy-oriented and contributes very little to the application and development of International Relations theory (Eriksson and Giacomello, 2006, p. 223; Dunn Cavelty, 2013). There are two reasons for this theoretical deficit. The first is the insufficiency of data required to systematically study cyber conflict, cyber capabilities, and cyber policy (Liff, 2012; Lindsay et al., 2015, p. 337). This limitation has prevented thorough empirical analysis and the development of theoretical propositions. The second reason is the inscrutability of studying cyber technologies. The technical nature of the information systems and computer protocols has made the study of cybersecurity more perplexing, but it has also motivated International Relations scholars to start theorising about the dynamics of cyber interactions (Valeriano and Maness, 2015, pp. 33-37). Currently, the analysis of cybersecurity issues has been left to certain policymakers who have contributed to the unnecessary securitization of cyberspace (Dunn Cavelty, 2008), as well as technologists who offer overly technical interpretations that are unhelpful in explaining the causes and consequences of cyber conflict (Kello, 2013, pp. 16-17).

Moving beyond these limitations, this study draws on the theories of International Relations to develop a more nuanced and compelling explanation for establishing the conditions necessary for the development of cyber capabilities in small states. It contributes to theory development is two ways. The study first tests the explanatory power of neo classical realism in analysing the foreign policy behaviour of small states. The framework follows deductive logic in evaluating whether the general assumptions, developed through collaboration between neoclassical realism (NCR) and strategic culture, can explain why New Zealand and Singapore have developed advanced cyber capabilities and why Brunei has not.  NCR as a framework is more progressive compared to other theories because it posits the distribution of power as an independent variable, but overcomes the analytical limitations of neorealism by including internal factors in its analysis of foreign policy (Rose, 1998).

The study then makes a second contribution by incorporating strategic culture as an intervening variable in explaining the foreign policy of small states. Culture in this context is a supplementary condition that bridges the gap between the systemic and state-level of analysis. The study contends that the distribution of power in the international system influences the development of cyber capabilities in New Zealand and Singapore, but only if their respective strategic cultures are oriented towards the use of networked-enabled technology. This inclination towards cyber capabilities can be explored by tracing the states' sources of strategic culture, specifically in terms of technology, history and policy. While previous research indicates strategic culture can independently influence foreign policy, it is considered as a secondary variable in the study (cf. Snyder, 1977; Hudson, 1997; Glenn et al., 2004; Farrell, 2005).

This chapter presents the theoretical framework that guides the rest of the study. It is divided into three sections and a conclusion. The next section discusses the levels of analysis, and situates cyber capabilities as a foreign policy instrument of states. The second explores the explanatory power of neoclassical realism by drawing out relevant themes and distinguishing the theory from alternative paradigms used to explain cyber phenomena. The third section presents the operationalization of the framework, particularly the variables, measurements, and limitations. The last section summarises the key points of the chapter.

## Levels of analysis

Building on the literature on cybersecurity and foreign policy, the study makes use of Rosenau's (1980) comparative foreign policy approach to explain the factors that influence the development of progressive cyber capabilities in New Zealand and Singapore, but not in Brunei. Rosenau (1980, pp. 115-159) suggested that explanatory factors are needed to account for the foreign policy behaviour of states, and he organised these factors according to five levels of analysis: system, role, government, society, and individual. This study adopts a modified version of this framework based on the work of Waltz (1979/2010) and Hey (2003) that suggest that role, government and society can be analysed at the state-level. Consequently, the study proceeds to analyse foreign policy at three levels: system, state, and individual.

An analysis of small state foreign policy, using a single level of analysis, is limited for several reasons. First, system-level explanations are limited because they predominantly focus on evaluating the foreign policy behaviour of great powers and downplay state-level factors, such as military organizational practices, that can influence the development of cyber capabilities. Moreover, while system-level explanations can account for the military build-up and foreign policy alignment of small states, these explanations were not designed to include state-level factors that are important understanding why some small states have employed networked technology as instruments to advance foreign policy.

Second, state-level explanations are important for small states however, these are also limited because they do not consider the dynamic external environment in the Asia-Pacific that shapes the strategic preferences of small states (cf. Hey, 2003; Alons, 2007). Lastly, there is little evidence that demonstrates the independent explanatory power of individual level explanations, such as elite preferences in influencing the foreign policy behaviour (Williams, 2012; Gvalia et al. 2013), while there is no evidence that links individual explanations to the institution of cyber capabilities of states (Kramer et al., 2009; Valeriano and Maness, 2015).

In accounting for the complexity of foreign policy analysis, the study employs NCR since it incorporates both external (systemic) and internal (domestic) variables, refining insights drawn from realism (Rose, 1998). Specifically, the framework "posits an imperfect transmission belt between systemic incentives and constraints" and the actual diplomatic, military, and foreign economic policies implemented at the state-level (Lobell, et al., 2009, p. 4). Strategic culture in this study is used as an intervening, state-level, variable that supplements the distribution of power argument provided by NCR. Culture is therefore considered a variable that can influence state preferences, but is treated as an "epiphenomenal" or secondary condition to international systemic constraints (Glenn, 2009, pp. 531-533).

*Role of strategic culture*

Strategic culture, as an analytical concept, has been an influential factor in shaping national security and foreign policy in the Asia-Pacific (Booth and Trood, 1999). The debates about how to define and utilise the concept are comprehensive, and have endured for several decades (cf. Gray, 1981; Johnston, 1995; Glenn, et al., 2004; Lantis, 2013). This study however, does not engage with these debates since the task of developing the concept is outside the scope of research. Instead, the study draws on the work of the "third generation" strategic culture scholars who argue for the significance of measurement in evaluating the effects of strategic culture on foreign policy (Johnston, 1995, pp. 41-43). Measuring the observable implications of strategic culture is useful because it clearly delimits the difference between cultural and non-cultural variables and makes the concept falsifiable when tested against other variables (Johnston, 1995, p. 45).

In this context, strategic culture is defined as "A distinctive body of beliefs, attitudes and practices regarding the use of force, which are held by a collective (usually a nation) and arise gradually over time, through a unique protracted historical process" (Longhurst, 2004, p. 17). Based on this interpretation, strategic culture can be traced by investigating the origins and evolution of state's strategic beliefs and practices within a given time frame, consistent with previous works on strategic culture.[7] For instance Johnston's

[7] The methodology of studying strategic culture is a subject of extensive debates that have not been resolved. Previous works that argue that strategic culture cannot be rigorously observed and measured include Snyder (1977), Lord (1985), and Gray, (1981, 1999). Scholars that challenge this view include Legro (1994), Johnston (1995, 1996, 1998), and Kier (1995). This study builds on the latter group of scholars and substantiates the concept of technology-oriented strategic culture through three observable implications: technological orientation, modernisation of the military and national security policies.

(1996, p. 216) pioneering study on Chinese strategic culture showed that the state "historically exhibited a relatively consistent hard realpolitik or *parabellum* strategic culture that has persisted across different structural contexts." Another important work that traces the evolution of a state's strategic beliefs and practices is Kier's (1995) study on the doctrinal developments in French Army. The study confirmed the influence of organizational culture on decision of the French Army to shift from offensive to defence doctrine during the period of 1919 to 1939.

The definition presented by Longhurst (2004) is therefore appropriate because it reinforces the study's objective of analysing the strategic culture of small states by tracing the evolution of the states' strategic beliefs and practices within a given time period. Based on this definition, strategic beliefs can be assessed through the significance that military organisations place on technology; attitudes towards technology can be evaluated by looking into the network readiness of states; and practices can be identified by evaluating the relevance of cyber conflict as a foreign policy priority. The operationalisation of these implications is discussed in a subsequent section of this chapter.

Consistent with this logic, the study assigns strategic culture as an epiphenomenon or secondary condition for two reasons. Firstly, previous studies indicate the strength and consistency of material capabilities, over cultural variables, in shaping military strategy and foreign policy the Asia-Pacific (Ross, 2006; Weatherbee, 2014; Tan, 2014; Glaser, 2015; Rosato, 2015). Although there are prominent studies that stress the prevalence of cultural factors, these examine a limited number of cases that do not represent foreign policy behaviour in the region (cf. Katzenstein, 1996; Peou, 2002). Secondly, strategic culture is treated as a condition that is necessary for the development of cyber capabilities, and not a variable that independently influences foreign policy. This distinction is crucial because culture as a secondary condition has limited influence as it can only affect foreign policy *if* the condition exists within an external environment constrained by the relative distribution of power. Strategic culture is therefore best understood as a complement to structural conditions that affect foreign policy.

## Cyber capabilities as foreign policy instrument

In exploring the utility of cyber capabilities, it is useful to assess these capabilities as foreign policy instruments used by states to pursue their national interests. This idea is based on empirical research that suggests that cyber conflict is predominant between states with existing foreign policy disputes (Valeriano and Maness, 2014; Carson and Yarhi-Milo, 2017; Poznansky and Perkosky, 2018).). In this sense, there are two strategies that states have generally employed cyber capabilities to achieve foreign policy objectives. The first is the use of covert action against adversaries. Covert action is a state instrument designed to support foreign policy by influencing political, economic, or military environments overseas without revealing the role of the sponsoring state (Johnson, 1989, p. 19).

A number of activities are included as part of covert action, from propaganda to paramilitary activities but the role of computer network operations is still being debated. The discreet and near instantaneous nature of cyberspace, however, makes cyber operations an appropriate and distinct activity within the range of covert action. Cyber operations can support foreign policy by influencing outcomes during security dilemmas where diplomacy is not effective and military action is counterproductive (Brantly, 2014, p. 466). A prominent example of computer-driven covert action is the use of a malicious computer worm (i.e. Stuxnet) by the U.S. and Israel to disrupt the uranium enrichment program of Iran in 2010. The operation was evaluated as low risk because it involved minimal human deployments, and was also judged as useful even if the outcome did not result in consequential damage (Barzashka, 2013, p. 48).

Another example is the use of cyber capabilities as a form of covert action is the policy of strategic ambiguity. This policy is adopted by states to introduce uncertainty in the decision-making process by deliberately not clarifying their involvement in contentious security situations, such as the policy of the U.S. towards the Taiwan Strait. The use of cyber capabilities by the U.S. to convey displeasure or concern towards China's actions towards Taiwan supports the policy of strategic ambiguity because the discreet nature of cyber operations may conceal or at least limit the involvement of the U.S (Bolt and Brenner, 2004). In the event of attribution, it would be advantageous for China if it maintains the secrecy of the operation to manage escalation risk despite its strategic competition with the U.S. This "tacit collusion" between states demonstrates how adversaries can limit war by concealing activities from outside audiences (Carson, 2016, p. 141). In this sense, states can therefore pursue their foreign policy interests through cyber operations with minimal risk of involvement or visible commitment to the parties engaged in the conflict (Libicki, 2011). The use of strategic ambiguity has been limited, but the proliferation of cyber capabilities makes strategic ambiguity a favourable strategy for states entangled in sensitive foreign policy dilemmas but are unwilling to commit substantial resources.

The second is using cyber capabilities to deceive adversaries. Deception through cyberspace is a distinct option that can potentially be employed as a protective strategy for states. While this idea is difficult to test empirically, preliminary research suggests that two advantages can be drawn from using strategic deception (Gartzke and Lindsay, 2015). Deception can improve cyber defensive operations by creating traps such as installing malicious software (malware) in critical databases to trace and subvert attackers after they infiltrate computer systems. Specifically, states may encourage computer network exploitation by allowing access to terabytes of data, but deceive perpetrators by attaching sophisticated malware in the stolen data (Singer and Friedman, 2014, pp. 55-59). Another is using deception to improve deterrence in cyberspace. Applying technical countermeasures, such as broadcasting beacons that can entrap attackers and trace its location, as well as silent intrusion-detection systems that give clues to attribution, increase the threat of detection and retaliation for perpetrators, thereby discouraging subsequent attacks (McHugh, et al., 2000; Modi et al., 2013).

The functions cyber capabilities discussed in the preceding paragraphs suggest additional foreign policy options that can potentially support existing foreign policy tools such as diplomacy, political intervention, and military action. Even if these examples are circumstantial and possibly outliers, they demonstrate what is possible depending on the capabilities and intentions of small states. In this context, a more systematic discussion that defines the foreign policy functions of cyber capabilities for small states is presented in Chapter 6.

### *Cybersecurity challenges for small states*

Cybersecurity remains an emerging foreign policy agenda for small states (Archer, et al., 2014, pp. 30-31). Prominent cyber incidents involving Estonia and Georgia were influential in escalating cybersecurity as a policy issue because these events exposed the vulnerabilities of small states to computer network attacks. A few studies that analysed cybersecurity predicament of small states have emphasised several challenges for foreign policy (Ragnarsson and Bailes, 2011; Chong, 2012;

Crandall, 2013; Areng, 2014). The first challenge is the limited resources and military capabilities of small states. It would be disadvantageous for small states to make use of cyber capabilities in the same manner as great powers because in the event of conventional retaliation, these states would be overpowered. Whilst a conventional military response to cyber attacks remains unlikely (Gompert and Libicki, 2014), using cyber capabilities to pursue foreign policy objectives can still place small states in a precarious position, due to the limited resources and capacity to respond to intrusions by more powerful states. This challenge highlights the need to assess the strategic utility of cyber capabilities for small states. Considering the inherent material limitations confronting small states, how can they exploit cyber capabilities to advance their foreign policy interests? This issue is thoroughly addressed in Chapter 6.

The second challenge is the narrow focus of small state foreign policy. Small states are generally concerned with foreign policy issues within their immediate region, therefore the ubiquitous orientation of cyber intrusions poses significant security issues for these states because they do not have extensive political, economic, and military resources to contend with capable adversaries from multiple jurisdictions (Burton, 2013, p. 224). This challenge raises the question of how small states can manage cyber threats that go beyond the scope of their foreign policy interests. Since small states tend to engage with foreign policy issues that directly affect their national interests such as territorial disputes, addressing cyber threats that can emanate from multiple jurisdictions, remains a significant challenge. The manner in which small states develop cyber capabilities as well as adapt their foreign policy strategies to to address cyber threats is discussed in Chapters 4 and 5.

The third challenge is the reliance of highly networked small states on information and communications technologies. Twelve out of twenty of the most highly networked states in the world fit within the study's definition of small (Bilbao-Osorio, et al., 2014, p. 10). From a technical perspective, high dependence on networked-enabled technologies generates problems for small states for two reasons. The first is that the risks of cyber attacks are higher for small states that have more public services that are contingent on the Internet (Grauman, 2012, p. 48). The second is that the incapacity of small states to diversify their internal and external Internet connections that contributes to higher risk of computer network attacks. (Stapleton-Gray and Woodcock, 2011, pp. 52-53). This challenge accentuates the double-edged impact of network-technologies on the situation of small states. Whereas small states improve their network readiness to strengthen their economic growth and global engagement, increased connectivity makes them more vulnerable to a different types and levels of computer network. The rationale for strong technology dependence and the strategies that small states employ to manage cyber threats are systematically discussed in Chapters 4 and 5.

*Cyber capabilities and small state alignment*

The utility of cyber capabilities in supporting the alignment strategies of small states is largely hypothetical due to the lack of empirical data (Liff, 2012; Valeriano and Maness, 2015). There are very few cases of cyber conflict where a connection between the institution of cyber capabilities and the strategic alignment of states can be established, hence generalisations and inferences have not been generated at this point. Based on the realist-oriented literature on foreign policy, less powerful states employ three main strategies in response to great power behaviour: accommodation, self-reliance and opposition (Waltz, 1979/2010; Walt, 1985; Layne, 2006a) Following these strategies, existing research suggests that self-reliance (e.g. neutrality and transcending) and opposition (e.g. balancing) strategies have been linked to the development of cyber capabilities in small states (cf. Chong, 2012; Burton, 2013; Crandall, 2014; Archer, et al., 2014). There are no studies to suggest the connection between accommodation (e.g. balancing and engagement) and the development of cyber capabilities. However, the cooperation between small states such as Tajikistan and Belarus with China can potentially confirm this link. Both states have requested China's assistance in capacity building for countering cybercrimes as well as reaffirmed their alignment with the regional power (Gao, 2017; Sender, 2017).

The case of Switzerland is an example of the linkage between cybersecurity and its foreign policy alignment. Switzerland's strategy of neutrality is reflected in its cybersecurity strategy because it clearly prioritises the resilience of critical infrastructure and domestic security threats over computer network operations against other states (Swiss Federal Department of Defence, 2012, p. 28). The Swiss Federal Department of Defence manages the implementation of the strategy however, consistent with their neutrality posture, cybersecurity organizations are dominated by citizen conscripts since professional military personnel are focused on countering conventional air and ground attacks (Dunn Cavelty, 2014, p. 22). While the Swiss Federal Council deliberated on developing capabilities for defensive information operations, the plan was abandoned due to a number of reasons including "legal ambiguities, financial and personnel shortfalls, and political reservations", leaving the military marginalised in the Swiss cybersecurity organizational set-up (Dunn Cavelty, 2014, pp. 21-22).

Estonia is another prominent case that reveals a connection between cybersecurity and foreign policy alignment. Estonia's response to widespread cyber attacks that were linked to Russia in 2007, can be characterised as transcending, or the attempt to go beyond the normal limits of conflictual politics by creating some institutional arrangements involving formal rules and procedures to address the threat (Schroeder, 1994, p. 117). Specifically, Estonia's foreign policy strategy focusing on strengthening its collective security arrangements with NATO to ensure that it could sufficiently respond to future cyber incidents (Crandall, 2014, p. 37). Moreover, cybersecurity has become one of the key objectives of Estonia's foreign policy particularly with the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) in 2008, which has been used as a platform for the development and promotion of norms for cyberspace (Crandall and Collins, 2015, p. 17).

Aside from self-reliance strategies, small states have also used cyber capabilities to complement balancing behaviour against powerful states. Taiwan is one of the few examples of this case, since it intends to improve the current security situation in the Taiwan Strait but at the same time develop the capabilities to respond to any eventualities (Ding, 2004). Since the situation remains unpredictable, Taiwan has implemented a balancing strategy against China by upgrading its military force, refining its early warning capabilities, and strengthening its volunteer military system, among other measures (Taiwan Ministry of Defence, 2015, pp. 73-75). These initiatives however, have necessitated the reinforcement of information security measures since improving military capabilities, specifically in the area of command and control for joint operations and electronic warfare countermeasures, makes Taiwan more vulnerable to computer network attacks. This concern, and recent sophisticated cyber attacks originating from China, has compelled Taiwan to extend its cooperation with the U.S. by requesting regular participation in the most extensive cybersecurity exercise coordinated by the U.S. Department of Homeland Security: "Cyber Storm" (Gold and Wu, 2015).

The preceding discussion highlights how the development and employment of cyber capabilities supports the foreign policy alignment of small states. Whereas previous studies have argued that existing theoretical paradigms are not sufficient to account for cyber phenomena, this study challenges this misreading by using international relations theory to explicate the value of cyber capabilities for small states. The next section therefore, discusses the progressiveness and strength of NCR in the context of the main alternative theoretical paradigms - constructivist, liberalist and technologist - in explaining the conditions that influence the development of cyber capabilities.

## Analytical themes and alternative paradigms

### *Neoclassical realism: the logical extension of neorealism*

The logic of NCR starts at the same point as neorealism: structures shape the behaviours of states but do not determine them (Waltz, 2000, p. 24). Neoclassical realists share the same core assumptions as neorealists regarding the state, relative power, and the dominance of the anarchical structure, but are unconvinced that these elements are sufficient to explain state behaviour (Foulon, 2015, p. 3). NCR therefore extends the explanatory power of neorealism in two ways. First, the theory focuses on explaining the foreign policy of states, a contribution that neorealism cannot provide since it assumes that other than power distribution, all states are alike in the international system (Waltz, 1979/2010, pp. 93-97). In this sense, NCR is more progressive because it includes among other factors, intervening, state-level variables such as strategic culture (Snyder, 1977), military and state interests (Schweller, 1993) and state power (Zakaria, 1999) in its analysis of foreign policy.

Second, NCR accounts for deviation in the foreign policy of states that do not respond to the structural incentives predicted by neorealism. A key prediction of neorealism, for instance, is that less powerful states will balance or bandwagon with great powers to ensure their survival in the international system. Although this behaviour is prevalent in the literature, it is not always valid as discussed in the previous section. This inconsistency is reflected in several studies that looked into the foreign policy of medium and small powers and revealed that less powerful states choose to be self-reliant rather than balance or bandwagon with great powers (Williams, et al., 2012; Gvalia, et al. 2013; Lim and Cooper, 2015). To address this gap, NCR contends that state-level variables are important because these often influence states to adopt policies that are not suitable responses to systemic incentives. The theory posits a "state-level-mediating variable", between system and foreign policy dynamics, that clarifies how state-level variables influence governments in crafting foreign policy that responds to binding structural incentives (Foulon, 2015, p. 3).

### *Anarchic international system*

An analysis of state foreign policy in the Asia-Pacific, using a neoclassical realist lens, begins with the fundamental assumption that the region is characterised anarchy or the lack of central authority that controls the use of force between states (Waltz, 1979/2010, p. 88). Due to this structure, small states such as New Zealand, Singapore and Brunei are forced to rely on their own resources and capabilities for survival. Given these constraints, self-help is necessary for these states to improve their national security posture, particularly through the modernisation of military capabilities and enhancement of their security cooperation with more powerful states.

Even though these efforts are necessary, they also lead to increased uncertainty in the region. The development of enhanced military capabilities strengthens the national security of states, but at the time increases the prospects of unpredictable and aggressive state behaviour in the absence of a central authority. This unresolvable uncertainty, or the idea that states can never be confident about the current and future intentions of other states, is one of the factors that affect the formation of military strategies and foreign policies in the region (Booth and Wheeler, 2013, pp. 147-149).  This interpretation however, has been challenged by other theoretical paradigms on several grounds.

First, constructivists disagree that self-help follows logically from anarchy because self-help is an institution or idea generated by interactions between states (Wendt, 1992, pp. 402-403). Self-help is not a constitutive feature of anarchy, as presumed by realists, but a consciously shared idea that affects a state's security interests as well as the character of their interactions. States are therefore not compelled to act because of the anarchic structure, but because of intersubjectively shared ideas, norms, and values (Copeland, 2000, p. 187).

Second, liberalists charge that the overemphasis on anarchy reduces the general understanding of international relations because it overlooks the interdependence of actors in international relations (Milner, 1991, p. 82). Anarchy may be a dominant characterisation of the international system, but interdependence between states is also a key structural feature of the system because it reflects the dynamics of international relations where the actions of states are conditioned by other actors' behaviour. Moreover, interdependence emphasises the significance of communication and information exchange among states, a crucial aspect that can reduce the transaction costs in efforts to understand the true preferences of other states (Keohane, 1984, pp. 92-94).

The constructivist claim, that ideas and norms shape state foreign policy is valid, but not convincing when applied to interstate dynamics in the Asia-Pacific. Previous studies focusing on territorial and political disputes in the Asia-Pacific suggest that material incentives such as economic resources (Katagiri, 2015), military capabilities (Hartfiel and Job, 2007), technology (Goldman and Mahnken, 2004) and geography (Porter, 2015) are more dominant factors than ideas and norms in influencing states to enhance their military capabilities in the region. Although ideas and norms may have influenced the construction of a security community by ASEAN (Acharya, 2000), Japan's culture of anti-militarism (Berger, 1998) and China's militaristic behaviour (Johnston, 1995), these cases are outliers that do not represent foreign policy behaviour in the Asia-Pacific (Peou, 2002, pp. 207).

NCR is a stronger theoretical framework because it transcends the limitations of constructivism. First, the theory's emphasis on material capabilities over other factors, makes it more persuasive in explaining small state foreign policy and military strategy in a region driven by competition (Mahnken, 2012). Second, the theory's capacity to incorporate state-level variables, particularly the strategic culture of small states, makes it more inclusive since it considers ideas and norms along with material factors. Third, the theory can explain what constructivism cannot: uncertainty between states (Copeland, 2000).

Constructivism privileges social interaction between states as the main factor that shapes foreign policy. It does not, however, provide any clarification on how states cope with uncertainty when they encounter conflicting interests or have disputes. NCR is more useful in this regard because it offers some insight about uncertainty regarding the intentions and capabilities of states based on the foreign policy behaviour of states. The theory assumes that uncertainty is generated from the anarchic international system thereby allowing the study to draw out the necessary conditions that affect the foreign policy and strategic preferences of states in the region.

Although the liberal argument that interdependence is equally important as anarchy is justifiable, it is weak when applied to state foreign policy in the Asia-Pacific. There are two reasons for this assertion. The first is that interdependence as an assumption is not useful in elucidating the incidences of lying and deception in state relations. Interdependence can explain the mutual dependence of states in terms of economic and social interests, however, it cannot reconcile inconsistencies of state preferences such as China's declaration of a peaceful rise to power and its aggressive behaviour in the South China Sea, or Cambodia's preference to support China rather than stay neutral regarding territorial disputes in the region (Thayer, 2010).

The second, is that interdependence is underdeveloped in Asia-Pacific because regional institutions have limited impact on state behaviour. There are currently four institutions that include China and the U.S. in discussions regarding regional security issues: the ASEAN Regional Forum, the East Asian Summit, the ASEAN Plus Three Cooperation, and the Shanghai Cooperation Organisation. Even though these institutions have contributed to peace and stability in the region, existing studies submit that they continuously struggle to mediate great power relations and are ineffective in resolving certain types of conflict, such as territorial disputes (Beeson, 2009; Wesley, 2009). Considering these limitations, it would be disadvantageous for small states like New Zealand, Singapore and Brunei to rely on regional security institutions in the Asia-Pacific without clearly gaining any advantages that can strengthen their national security.

Given these limitations, NCR is more useful as a theoretical framework because it surpasses the weaknesses of liberalism. The first advantage of NCR is that it anticipates lying and deception between states because of the lack of a central authority in the Asia-Pacific (Mearsheimer, 2010, p. 8). Anarchy compels states with different military capabilities to be vigilant about the intentions and postures of neighbouring states in the region. The second advantage is that the theory diminishes the significance of non-state actors, particularly international institutions, in influencing state foreign policy. NCR posits that states are the primary actors in the international system, therefore the theory is more appropriate when applied to foreign policy behaviour because of the dominance of states over institutional influence in the Asia-Pacific.

*Relative distribution of power*

As a consequence of an anarchical environment, neoclassical realists contend that various distributions of power emerge in competitive relations between states. This is manifested in the disparity between the military capabilities of states in the Asia-Pacific Region as well as the increasing, arms transfers and military expenditures by middle powers and small powers including India, Australia, South Korea, and Vietnam (Bitzinger, 2010; Tan, 2014; Fleurant, et al., 2015). The discrepancy in military capabilities has extended to cyberspace, where great powers have exploited computer networks to support foreign policy objectives in the region (Valeriano and Maness, 2015). A range of attack methods, employed by China and North Korea in relation to political and territorial disputes, has compelled some less powerful states to develop cyber capabilities to improve their defensive capabilities.

In this context, the imbalanced distribution of military capabilities within the region is the primary incentive for the enhancement of military capabilities, including the development of computer network operations as a crucial component in building a superior military force. While the relative distribution of power is a sound argument, scholars that identify with other theoretical paradigms contest the analytical value of this concept. Liberals dispute the influence of the relative distribution of power as a condition that drives the interaction of states, while technologists accentuate the role of information and communication technologies in influencing the different aspects of government and society.

Liberals are not satisfied with the relative capabilities argument presented by NCR because they contend that this does not accurately represent the interactions between states. They maintain the framework of complex interdependence is more persuasive because it characterises interactions among states by defining multiple channels of relations, the absence of a hierarchy of issues, and the minor role of the military (Nye and Keohane, 2012). In explaining cyber interactions, liberals would emphasise the centrality of complex interdependence between states as a main driver of state behaviour. When applied to the Asia-Pacific, complex interdependence would focus on the multiple channels that connect states and non-state actors through cyberspace at different levels between governmental elites, multinational firms, and civil society. Liberals would contend that non-military issues such as health and education should be given the same priority as cyber threats in the decision-making process. Lastly, they would highlight the lesser role of military force due to the decrease of interstate conflict and the increase of mutual influence among states through technology (Nye and Keohane, 1998). While liberals contend that the framework of complex interdependence is a more potent alternative to the distribution of power, technologists emphasise the role of technology in changing the interactions between actors in the international system.

Technologists challenge the logic behind the relative distribution of power because they argue that technology, not the power relations between states, is the driving force that influences society and consequently the preferences of states. This view is anchored on technological determinism, a theory about the relationship between technology and society. The theory makes two central claims: "the development of technology proceeds in an autonomous manner, determined by an internal logic independent of social Influence" and technological change determines social change in a prescribed manner" (Kline, 2001, p. 15495). While the theory does not directly address the development of cyber capabilities, its focus on technology makes it relevant to the subject of inquiry.

The rigid version of this theory suggests that the development of cyber capabilities is consistent with the development of new technologies (Raudzens, 1990). This view is substantiated by previous studies that stress the strong potential of information and communication technologies in producing outcomes during warfare (Arquilla and Ronfeldt, 1993; Nye and Owen, 1996). The more flexible version, or "soft determinism", argues that historical events do not strictly dictate subsequent technological developments but at least make "sequences of technological improvements in one direction easier" (Rosenberg, 1994, p. 15) In this interpretation, the influence of global networks enables unparalleled economic transactions and encourages governments to "share sovereignty" through integration and engagements with international institutions, but does not independently force change in society (Castells, 2000, p. 155).

The concept of complex interdependence is useful but it overlooks crucial issues that affect state interactions in the Asia-Pacific. The characterisation of multiple channels does not consider why, despite the extensive connections between states, computer network attacks are still prevalent not only against government targets but also against multinational firms and civil society organizations. Non-military issues, particularly natural disasters and overpopulation, may have substantial weight in Asia-Pacific, but the continuous increase in military expenditures in the region and the substantial arms transfers between states, confirm the prioritization of military force development. The drive to improve military capabilities also invalidates the idea that the military has a diminished role in state relations because states remain insecure despite the prevalence of networks and connection.

Given these issues, NCR is a stronger theoretical framework for two reasons. First, the theory treats state relations as superficial because dependence on other states is just a strategy to survive in an anarchic international system. This assumption is beneficial since it anticipates negative interactions among states, such as deception and conflict as part of international relations. Second, the theory's focus on national security as the primary issue in policy-making makes it more appropriate in explaining cyber conflict and the development of cyber capabilities in the Asia-Pacific Region.

The idea that that technology is the driver of change in society or technological determinism is a credible, but ultimately unsatisfying when applied to the foreign policy predicament of states in the Asia-Pacific. The first limitation is that the theory does not account for uneven distribution of technological capacity between states. The majority of the states in the region are still in the process of developing cybersecurity measures, let alone computer network operations, therefore few have actual national strategies for cyberspace (Feakin, et al., 2015). Technologists assume the decisive role of information and communication technologies in shaping state behaviour, but they do not explain why less developed states, such as Cambodia, Laos, and the Philippines, have underdeveloped ICT infrastructures and minimal capabilities for military operations in cyberspace. NCR builds on the limitations of technological determinism by emphasising the asymmetrical distribution of capabilities as a central factor that directs states to contemplate the use of cyber capabilities as one of the options to achieve foreign policy objectives.

The second limitation is that technological determinism understates the consequences of the increased reliance on ICTs. Technologists fail to highlight the double-edged effect of technology: the advantages afforded by technology also create vulnerabilities. This critical point is reflected in the growing literature that stresses the limitations of networked-enabled technologies in achieving military outcomes and foreign policy objectives (Gray, 2010; Valeriano and Maness, 2015). NCR, exceeds the explanation advanced by technologists by treating technology as a means to enhance national security and manage foreign policy objectives. Following this argument, the theory treats the prevalence of cyber conflict as an extension of conventional military operations, and the development of cyber capabilities as a manifestation of capability alignment for states to protect their national interests in the region.

*Bridging two levels*

Structural approaches to explaining foreign policy are limited because these do not include state-level or domestic factors in its analysis, while state-level factors alone are insufficient and provides less sophistication in explaining foreign policy (cf. Singer, 1961; Rosenau, 1969, Evans et al., 1993). These observations are more acute for cyber conflict because it pervades all levels of interaction in the international system. In this sense, a logical approach is to address the dilemma and evaluate foreign policy from two levels of analysis: systemic and state. Since this study treats cyber capabilities as a foreign policy instrument, it is important to note that individuals have limited influence over the creation and advancement of computer network capabilities because of the time and enduring organisational resources required for operationalisation (Denning, 1999; Rattary, 2001; Healey, 2013).

Existing literature in International Relations offers two main approaches that combine systemic and state-level explanations. The first is NCR, which is the theoretical framework of the study, and the second is the Two Level Game

(TLG) approach developed by Putnam (1998). There are three overlapping claims that make the NCR and TLG useful for the study. First, both approaches explicitly combine systemic and state-level factors in analysing foreign policy (Foulon, 2015, p. 6). Second, both respond to the deficiencies of earlier approaches that ignore the influence of state-level factors (Pastor, 1993, p. 327). Third, both approaches capture the interaction between international and domestic politics, allowing for a more detailed understanding of state behaviour (Schweller, 2003).

Although these features are constructive, NCR is the superior theoretical framework for the study. There are four justifications for this assertion. Firstly, NCR is oriented towards military and security issues (Schweller, 2003), whereas TLG prioritises diplomacy and economic concerns (Putman, 1998). Secondly, NCR clearly delineates the systemic level as the leading factor in analysing foreign policy, while TLG is not clear on which level is more dominant (Foulon, 2015, p. 7). Thirdly, NCR establishes the theoretical link between the systemic and state-level as an "imperfect transmission belt" (Lobell et al., 2009, p. 4); a stark contrast to TLG, where the connection between the two levels is not clearly established (Putnam, 1988, p. 456). Lastly, previous studies indicate the productive application of NCR combined with strategic culture as a state-level variable in explaining foreign policy preferences (e.g. Snyder, 1977; Dueck, 2005; Glenn, 2009), however this collaboration has not been established using the TLG approach. Building on these advantages, NCR is therefore the most appropriate theoretical framework for the study.

## Neoclassical realism as an explanatory framework

The study seeks to develop a more refined understanding of the strategic utility of cyber capabilities as a foreign policy instrument for small states in the Asia-Pacific. In addressing this objective, the explanatory framework in this research explores the association between variables by identifying the necessary conditions for developing cyber capabilities. Since the objective of study is to understand *why* small states develop cyber capabilities, it does not intend to establish the degree of relationships between variables nor determine the causes of cyber conflict in the region.

*Framework for necessary conditions*

The study hypothesizes that there are two necessary conditions for the development of cyber capabilities in small states: distribution of power and strategic culture. Following the framework of NCR, the distribution of power in the region is the independent variable or dominant condition that is filtered by strategic culture, an intervening variable or secondary condition that adjusts the foreign policy preferences of small states towards the development of cyber capabilities.  Figure 1 presents the conceptual framework of the study and indicates a linear association between variables. This framework makes two claims. The first assertion is that the distribution of capabilities affects the strategic culture of small states. This is based on the logic that the strategic culture of small states is influenced by the significant disparity between military capabilities since these states have fewer material resources and are on the weaker side of the competition. This is reflected in Figure 1 through the first arrow that indicates the relationship between the distribution of power and strategic culture. This imbalance is more prominent in terms of cyber capabilities, particularly given that the most active states in the cyber environment all have foreign policy interests in the Asia-Pacific. The second assertion is that both external and internal conditions must be present for the small states to consider cyber capabilities as a foreign policy instrument. This assumption is based on research that shows that the external factors alone cannot influence states to make use of cyber conflict as a strategy without existing state-level preconditions (Rattray, 2001; Denning, 2003). This is reflected in Figure 1 through the second arrow that suggests that the combination of factors - distribution of power and strategic culture – are necessary for small states to consider cyber capabilities as part of the foreign policy arsenal that is essential for managing the geopolitical conditions in the region.

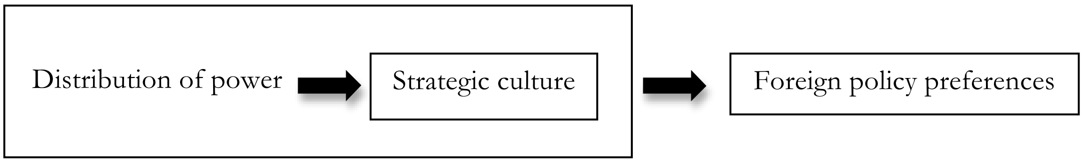


Figure 1: Conceptual framework

In applying the conceptual framework, the distribution of power can be specified as the imbalanced distribution of military capabilities between states in the Asia-Pacific. This phenomenon is examined through an evaluation of three observable implications in each state: great power rivalry, military expenditures, and arms transfers (Gray, 1971). Strategic culture on the other hand, is explored through an assessment of three observable implications in each state: technological orientation, modernisation of the military and national security policies. While there are various sources of strategic culture, these three implications have been selected based on previous studies that point out that technological orientation, military modernisation, and national security policies are shaped by history and are dependent on events that set "into motion institutional patterns or event chains that have deterministic properties" (Mahoney, 2000, pp. 507-508). First, in assessing technological orientation, Herrera (2006, pp 3-5.) argues that evolution of "sociotechnical systems" such as the railroad and atom bomb, can be observed through deterministic historical patterns.

Second, in terms of modernisation, previous studies, suggest that historical experiences affect the military's preference for adopting emerging technologies. For example, Adamsky (2010, pp. 46-48) argues that Russia's intellectual traditions and practices influenced the state's inclination for "self-conscious conceptualization," which influenced the use of terms "Revolution in Military Affairs" and "Military-Technological Revolution" to describe radical shifts in the ways and means in waging war. Moreover, Raska's (2011, pp. 216-217) work on military innovation in small states suggest that the historical experiences of South Korea and Israel have compelled them to search for "new security paradigms that would enable "greater flexibility, adaptability, and autonomy under conditions of strategic uncertainty." In this context, both states explored the integration and exploitation of new generation RMA-oriented technologies in modernizing their respective military forces.

Third, it is possible to extend the path-dependent logic to the development of national security policies. For instance, in studying Germany, Banchoff (1999) posited that the evolution of its foreign policy was shaped by both historical memory and geopolitical conditions. More recently, Haglund (2014) argued that security policies in the Asia-Pacific are shaped by strategic beliefs and practices a follow path-dependent logic. Based on these assessments, this study argues that a state's technological orientation or preference for harnessing networked technologies is influenced by its previous experiences that were consequential to its national development. Figure 2 presents the applied framework of the study in which strategic culture must be present, within a binding geopolitical environment, to create conditions for the development of cyber capabilities as a foreign policy instrument for small states.

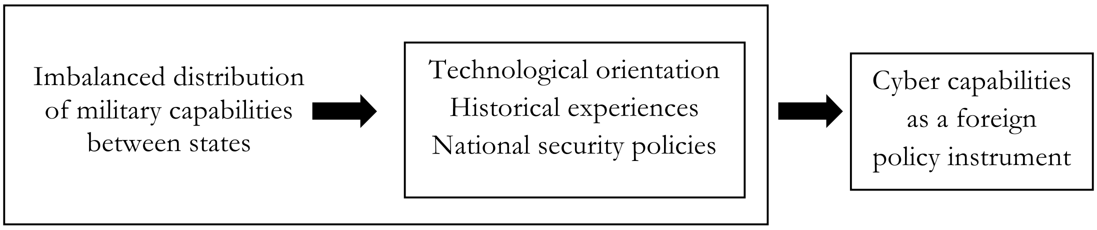

Imbalanced distribution of military capabilities between states
Technological orientation
Historical experiences
National security policies
Cyber capabilities as a foreign policy instrument

Figure 2: Applied framework of the study

The application of the framework must also clarify how the observable implications will be measured for each variable. The relative distribution of military capabilities (independent variable) is measured through a combination of quantitative and qualitative data: the number of great powers, the increase in military expenditures, as well as the direction of arms transfers in the region. Strategic culture (intervening variable) is also measured through a collaboration of quantitative and qualitative data: network readiness, the importance of technology in military operations and the relevance of cyber conflict and threats in national security documents. A summary of the observable implications and measurements is presented in Table 3.

| **Variables** | **Observable Implications** | **Measurements** |
|---|---|---|
| *Distribution of power* | Great power rivalry | ‣ Number of great powers that have interests in the region<br>‣ Evidence of cyber conflict |
| | Military expenditures | ‣ Increase in military spending<br>‣ Evidence of expenditures for cyber capabilities |
| | Arms transfers | ‣ Increase in the transfer military weapons<br>‣ Evidence of cyber capabilities |
| *Strategic culture* | Network readiness | ‣ Measurement of environment, readiness, usage, and impact of ICT by the WEF |
| | Relevance of technology for military affairs | ‣ Indications of a technology-driven modernisation<br>‣ Evidence of military upgrades focused on cyber capabilities |

| | | |
|---|---|---|
| | Relevance of cybersecurity | ‣ Recognition of cyber threats as a national security issue<br>‣ Existence of an official strategy for addressing cyber threats |

Table 3: Observable implications and measurements

*Counterarguments and hypothesis testing*

A crucial aspect of applying theoretical frameworks to structure the analysis of the study is to recognise the limitations in explaining foreign policy behaviour. This assessment can be strengthened by engaging with the counterarguments to the study's prevailing assumptions and by demonstrating the falsifiability of the hypothesis or central argument. The arguments that challenge the hypothesis of the study can be divided into two levels. The first set of counterarguments focus the systemic or structural level of the framework. The main counterarguments against the realist interpretation of the structural conditions in the region has been discussed systematically in the previous sections of this chapter but a brief summary would be useful. The distribution of power is the primary necessary condition in the study because it can account for the geopolitical realities in the Asia-Pacific Region. Cyber conflicts do not exist in a vacuum; they occur because of the prevailing structural conditions that shape the offline and online interactions between states. As discussed in the previous sections, alternative structural theories such as neoliberal institutionalism, social constructivism, and technological determinism can provide valid insights about the structural condition in the region, but they do not accurately reflect the geopolitical realities and the cyber interactions in the region.

The second aspect is the state or domestic level of the framework. The main counterarguments against strategic culture being the domestic factor has been mentioned in the previous sections of the chapter but a more detailed discussion is warranted here to clarify the connection between strategic culture and the development of cyber capabilities. Strategic culture is the secondary necessary condition in the study because this variable signifies the preference of small states to fully engage with networked technologies. This preference is captured in the concept of technology-oriented strategic culture or the tendency of small states to depend on digital technology to enhance their strategic options (see Chapter 5). The literature on foreign policy analysis presents three alternative frameworks that focus on the domestic level analysis: governmental politics, new liberalism and individual perspectives (Carlsnaes, 2016, pp. 121-124).

The bureaucratic or governmental politics is one alternative framework that examines domestic level factors. This framework underscores the role of bureaucratic infighting, government process, and the interaction of individuals within their organisational environments, as the main factor that affects foreign policy behaviour of states (Allison and Zelikow, 1999, pp. 255-256). In applying this framework, foreign policy scholars could potentially draw on the competition between the intelligence and defence communities for authority over cyber operations as the main factor that compels the government to strengthen its capacity for cyber operations, as discussed in Samaan's (2010) work on the U.S. Cyber Command. While this framework has potential, it fails to account for the impact of the uneven distribution of capabilities between states. Powerful states such as the U.S. and the UK have well-resourced and highly capable government agencies yet, they seek to collaborate with different sectors of society in countering complex cyber threats (The White House, 2011, p. 11; UK Cabinet Office, 2016, p. 26). It is unrealistic for government agencies of small states to independently influence the development of cyber capabilities for of two reasons. First, the government lacks the expertise and capacity to address cyber threats without support from the private sector and civil society organisations (Carr, 2016). Second, networked technologies are utilised by all sectors of society therefore the securitisation of cyberspace or even the regulation of network technologies by the government will have unintended consequences that can implicate private companies and the civil society organisations (Dunn Cavelty, 2008). The fallout between the U.S. and its allies regarding the state's global mass surveillance activities is a prominent example of the dangers of unilateral government initiatives to developed more advance cyber capabilities. For these reasons, governmental politics is an insufficient domestic variable to supplement the relative distribution of power within the explanatory framework of the study.

New liberalism is another alternative framework that analyses domestic factors. The framework emphasises the primacy of societal actors such as individuals and private groups as the main factor that influences the foreign policy behaviour of states. Based on this approach, foreign policy scholars could establish that societal actors such as private companies (Hare, 2009) and prominent technologists (Hurel and Lobato, 2018; Hoffman, et al., 2018) can influence states to develop the capability to defend state interests in cyberspace.

Societal actors may have the expertise and resources to leverage the advantages of networked technologies but they lack the authority and legitimacy to advance the national security interests of the state (Dunn Cavelty and Suter, 2009; Carr, 2016). While strong public-private partnerships are indispensible for building a robust cyber strategy, these arrangements are managed to serve the agenda of the state. A key example that illustrates this point is the exploitation of social media platforms for intelligence collection by the U.S. and UK (Bauman, et al., 2014; Walsh and Miller, 2016). In this context, new liberalism is an inappropriate domestic variable that compliments the distribution of power because the government and not societal actors are ultimately responsible for protecting the national security of the state.

The perspectives of individual actors are the third alternative framework that advances domestic factors as a source of foreign policy influence. This framework focuses on the ideas, beliefs and preferences of leaders and political elites within a state. The cognitive and psychological approach within this rubric, examines how characteristics of leadership, beliefs, motivation, decisional, and interpersonal styles affects the pursuit of foreign policies (Herman and Preston, 2004, pp. 363-369). This also includes small-group approaches that investigate the effects of groupthink on flawed foreign policy decisions in times of crisis (Janis, 1972), prospect theory which "points to deviations from expected utility theory, the conventional means of explaining choice under conditions of risk" (Kahler, 1998, p. 982), and the interpretative perspective that considers the thinking and actions of individual decision makers as the source of foreign policy behaviour (Carlsnaes, 2016, p. 124).

Although these approaches offer detailed explanations about the role of individual actors, there are two reasons why they cannot account for the use of networked technologies as a foreign policy instrument. The first reason is that networked technologies are pervasive so they cannot be managed or controlled by individuals. State leaders and political elites can enact policies that require the use of network technologies but the adoption and implementation of these policies involve the participation of a range of actors across different sectors society. A counterargument to this point might be the case of authoritarian regimes such as

North Korea, where government has total control over all the instruments of the state including the development and use cyber capabilities (Jun, et al., 2015). This argument is valid, but it is not applicable to the study considering that North Korea is an extreme outlier state.  The second reason is that state leaders and political elites will be constrained from prioritising cybersecurity particularly when their respective states do not have the capacity, resources, and infrastructure for building a networked society. These underdeveloped states are affected by "digital pitfalls" such as a weak technological environment, lack of cybersecurity strategy and policy, and poor network infrastructure, all of which are necessary for adapting to the information age (Schia, 2018, pp. 826-830). Consequently, state leaders and political elites of these states will have to focus on more vital national issues such as crime, poverty, political violence, and overpopulation among others, if they want to remain in power. Based on these considerations, the preferences of individual actors are insufficient to supplement the relative distribution of power because state leaders and political elites do not have control or even manage the emergence and use of network technologies in domestic affairs.

The substantial counterarguments examined in the previous sections of this chapter represent the alternative hypotheses of the study. These hypotheses were rejected because the arguments they advance are inappropriate for the study and empirical evidence presented to support these hypotheses are also weak. In these sense, the study hypothesises that the imbalanced distribution of power and a technology oriented strategic culture are *necessary but not sufficient* conditions for small states to develop cyber capabilities. While network defence is a fundamental reason why less small states states develop cyber capabilities, the active skirmishes between different "cyber powers" in the region have compelled small states to respond to the new environment and pursue more strategic options by developing the capacity for computer network operations. A technology oriented strategic beliefs and practices play a role in the strategic calculus of small states because they direct the preferences of these states towards the use of networked technologies to advance their national interests.

Table 4 presents a summary of alternative hypotheses and the justifications for rejecting them. The falsifiability of the theoretical framework was demonstrated through the inclusion of Brunei as a negative case. In contrast to New Zealand and Singapore, Brunei does not have a technology oriented strategic culture because of the state leadership's apprehension about the potential of technology to facilitate the ideas that challenge the beliefs and practices advocated by its national ideology of Malay Islamic Monarchy. The argument is analysed thoroughly in Chapter 5.

| Variables | Alternative Hypotheses | Basis of rejection |
|---|---|---|
| *System level/Structural* | Ideational factors influence foreign policy behaviour (constructivism) | 1. The theory's focus of ideas and norms as the source of foreign policy behaviour is weak when applied to the Asia-Pacific Region. |
| | Complex interdependence between states influences foreign policy behaviour (liberalism) | 1. The theory cannot account for incidences of lying and deception between states.<br>2. The theory's emphasis on the impact of international institutions in moderating state behaviour is weak when applied to the Asia-Pacific Region.<br>3. The theory cannot explain why computer network attacks continue to be prevalent despite extensive networks between states. |
| | Technology is the driver of foreign policy behaviour (technological determinism) | 1. The theory is inappropriate because does cannot account for uneven distribution of technological capacity between states.<br>2. The theory understates the consequences of the increased dependence on network technology. |
| *State level/Domestic* | Governmental politics | 1. The framework is inadequate because it cannot account for the impact of the unequal distribution of capabilities between states. |
| | New liberalism | 1. The theory is inappropriate because it privileges societal actors that lack the authority and legitimacy to advance the national security interests of the state. |
| | Cognitive and psychological approach | 1. Individual approaches are deficient because networked technologies cannot be managed or controlled by individuals.<br>2. Individual approaches are insufficient because state leaders and political elites cannot prioritise the development of cyber capabilities if they are constrained by the digital divide. |
| | Interpretative approach | |

Table 4: Summary of alternative hypotheses

*Technology and the distribution of power*

Technology is a decisive element that contributes to the shifts in the distribution of power within the international system (Krause, 1992, p. 19). States that have access to advanced military-relevant technologies can develop more effective weapon systems that are vital for a potent military force, which in turn facilitates the projection of greater geopolitical power (Bitzinger, 2016, p. 1). In this sense, cyber capabilities are crucial instruments for states in the Asia-Pacific because of the heightened geopolitical rivalry between great powers, the proliferation of advanced conventional military weapons, and the need to secure non-government interests in cyberspace.

The geopolitical rivalry between China and the U.S. for power and influence in the Asia-Pacific is a decisive factor that contributes to the importance of cyber capabilities. This predicament has manifested in different facets of state interaction, most prominently in the military domain, where China has been rapidly modernising its military forces in an attempt to catch up with U.S. military superiority. While China's conventional military build-up is well documented, its proven capacity to engage in computer network operations against complex targets, such as the U.S. Department of Defense and Foreign and Commonwealth Office of the United Kingdom, has attracted more apprehension from policymakers, making it a main actor in perpetuating cyber attacks in the region (Valeriano and Maness, 2015, p. 128). The U.S. response to China's activities in cyberspace has been comprehensive: elevate cybersecurity as a national security priority; strengthen its organisational and operational capacity to engage in computer network operations; and demonstrate the capacity to execute cyber attacks against adversaries.

The persistence of both states in actively engaging in computer network operations, in support of their foreign policy objectives, has extended their rivalry in cyberspace thereby enhancing the role of military forces in cyber operations (Domingo, 2016). Moreover, this competition has introduced computer network operations as a normal or status quo capability in military conflict, which has influenced other states in the region to develop cyber strategies and capabilities.

Another factor that increases the importance of cyber capabilities in the region is linked with the spread of advanced conventional military weapons among medium and small powers in the region. Academics and security analysts have acutely observed the arms build-up for the past two decades, and there is an emerging consensus that the modernisation of warfighting capabilities of states is beyond the normal process of upgrading old equipment to new, more sophisticated weapon systems (Goldman and Mahnken, 2004; Ball, 2009; Bitzinger, 2010, 2015). The investment in modern capabilities, such as low observable technology (stealth) and standoff precision-guided weapons, is driven by a confluence of different internal and external factors that continue to influence the military strategies of states in the Asia-Pacific (Tan, 2014).

An important phenomenon that relates to the conventional weapons build-up is the prevalence of enduring interstate rivalries in the region. These conflicts have extended to cyberspace, compelling states such as South Korea to develop cyber capabilities to protect its critical national infrastructure against politically motivated computer network attacks by North Korea (Valeriano and Maness, 2015, pp. 128-129). India and Pakistan form another example of a regional rivalry where conflict has manifested into a number of cyber incidents. These circumstances have initiated debates about creating a more aggressive cybersecurity posture for India (Desai et al., 2012).

The increased reliance of military forces on networked-enabled military technology has influenced states to develop cyber capabilities to ensure that military networks that control and deploy modern weapons systems are not compromised. Indeed, cyber defence has been a strong motivation for secondary states to develop cyber capabilities in the region, considering that even military operations other than war (e.g. peace enforcement and humanitarian assistance) also necessitate advance military capabilities that are dependent on information and communication technologies (Betz, 2008). Given this conflict environment, cyber capabilities have therefore become a fundamental prerequisite for states deploying twenty-first century military capabilities.

The last factor that enhances the value of cyber capabilities for states is the need to protect non-government interests in cyberspace. The interests of other sectors such as private companies and civil society need to be protected by the state because these sectors contribute to the development of capacity, resources, and norms necessary for states to manage the power imbalance in the region as well as the insecurity in cyberspace (Harknett and Stever, 2009; DeNardis, 2014; Hoffman and Levite, 2017). Indeed, since network technologies have similar efficacy for military and civilian sectors, many technologies developed for civilian use will always have military potential in the areas of mobility, communications, and intelligence (Buzan, 1987, pp. 28-29). However, in this sense, the extensive application of network technologies across sectors has a doubled-edged effect because the security threats confronting the military sector can also affect the civilian sector and vice versa.

Although computer network operations are mainly applied for espionage, sabotage, and subversion against other states, these capabilities are also exploited for use in commercial environments. The accessibility of Internet-based, inexpensive computer tools that can target private sector assets is an emergent threat to the economic stability of highly industrialised states that depend greatly on information infrastructures. Business leaders are now confronted by analogous threats that states have been countering: cyber espionage, organised crime, perception battles, and infiltrations by hackers or groups supported by business competitors (Knapp and Boulton, 2006, p. 85). The pervasive nature of cyber threats therefore makes cyber capabilities inevitable tools for states to develop because it enables them to secure information networks and critical infrastructures that are decisive for states to defend their national security and manage the disparity in military capabilities between states in the region.

The competition between great powers, proliferation of advanced conventional military capabilities, and the need to secure non-military interests in cyberspace, contributes to the unequal distribution of cyber capabilities, which in turn affects the balance of power in the region. States that first exploited the advantages of cyberspace for strategic purposes have eventually dominated the new environment. China and the U.S. are the most powerful actors in cyberspace because of the considerable expertise, time, and resources they have devoted to developing capabilities for computer network operations (Domingo, 2016).

Medium powers like Australia, South Korea, and Japan do not have the same of level of capabilities and resources but are motivated to develop robust cyber capabilities to supplement their substantial investments in conventional military weapons. Finally, a majority of states in the region, including Malaysia and Indonesia, have developed defensive cyber capabilities specifically to protect non-military interests' such as transactions of the private sector and the conduct of trade and diplomacy with neighbouring states. These states are likely to be the weakest since their capabilities in both conventional and cyber military operations are limited relative to great and medium powers.

*Technology and strategic culture*

The distribution of power is a primary variable that facilitates the development of cyber capabilities in the region, but a state's strategic culture is instrumental in shaping how states make use of these capabilities as tools for achieving their foreign policy objectives. Strategic culture is a necessary secondary variable to consider in exploring the utility of cyber capabilities. It provides rational explanations regarding the beliefs, attitudes, and practices of states towards using information and communication technologies as an instrument of foreign policy in the international system. In this study, the concept of a "technology-oriented" strategic culture is introduced to characterise the tendency of small states to depend on technology as a strategy to compensate for limited resources, military capabilities, and strategic depth. Technology in this context is an enabler for states to pursue foreign policy objectives in a more decisive and calculated manner. A "technology-oriented" strategic culture can be observed through an assessment of three implications for small states: high network readiness, technology-driven military force and the relevance of cybersecurity for the state.

The first implication is high network readiness. This is a strong indicator of how states capitalise on information and communication technologies to enhance different functions across different sectors of society. Indeed, the WEF developed the NRI to measures the capacity of states to leverage information and communication technologies for increased competitiveness and well-being (Baller et al., 2016, p. xi). Network readiness is a key component of a technology-oriented strategic culture because it suggests a state's interest in investing a substantial level of resources and effort to develop a robust digital environment that contributes to the realisation of economic prosperity.

For instance, Australia, Singapore, Japan, Hong Kong, and South Korea are the most highly networked states in the region for the reason that they have managed to exploit the advantages of technology-driven industries such as professional services, finance and insurance, manufacturing, and media and telecommunications While network readiness can provide value insight into the technological preference of states, it also has limitations. One drawback is the fundamental dilemma of a networked society innovation: highly networked states are the most susceptible to cyber intrusions because of their reliance on information and communication technologies (Midgley, et al., 2016, p. 19). In this sense, the double-edged impact of information and communication technologies raises strategic challenges for highly networked states that drive the need for the development of a cybersecurity strategy and capabilities. Another limitation is that network readiness does not account for how states utilise or employ these technologies for strategic purposes. The data used for producing the NRI were collected from on surveys, which are designed to "assess the prevalence of attitudes, beliefs, and behaviors" (Weisberg, 2007, p. 223) of respondents regarding the use of information and communication technologies to enhance economic competitiveness and not necessarily national security. This limitation is the reason why other observable implications are included in evaluating strategic culture of small states.

A second implication for technology-oriented strategic culture is the emphasis of the state on a technology-driven modernisation for its military force. This idea draws from the vaunted theory of military transformation advanced by the U.S.: the Revolution in Military Affairs (RMA). The RMA theory is based on the idea that extensive changes in any number of variables of war will generate changes in the entire military organisational structure, doctrine, and operations (Loo, 2009, p. 4). While the RMA theory offers a compelling explanation for the instrumental role of technology in military affairs, the ideas espoused by this theory have not been readily accepted by states that do not have the resources, experience and knowledge to engage technology-driven modernisation (Loo, 2009; Raska, 2011; Domingo, 2014).

In response to the military transformation led by the U.S., not all states in the Asia-Pacific have engaged with ideas promoted by the RMA theory. The nonconformities in responses can be linked to differences in strategic culture, considering that preferences held by states are shaped through unique historical experiences and not necessarily shaped by great powers (Longhurst, 2004, 17). Tan's (2014) categorisation of state responses provides an accurate view of the situation in the region. He contends that there are three distinctive blocs of state responses: a loose RMA-oriented bloc of U.S. allies; a counter-RMA bloc of possible U.S. adversaries; and a neutral bloc of states with industrial age armed forces that seek gradual rather than radical military transformation (Tan, 2014, p. 157).

Following on this categorisation, it is likely that states with cyber capabilities are part of the three blocs specified by Tan (2014) due to their inclination towards military-relevant technologies. It is important to note however, that whilst these states derive strategic advantages from technology, the trajectory of their military modernisation and use of their military forces, are still determined by collective beliefs, attitudes, and practices shaped by historical experiences and geopolitical circumstances (Booth and Trood, 1999, p. 9).

The third implication for technology-oriented strategic culture is the relevance of cybersecurity for states in the region. The level of awareness by regional governments regarding threats and opportunities, derived from increased cyber engagement, remains uneven (Feakin, et al., 2015). This observation is manifested in two areas: recognition of the relevance of cybersecurity as a national security issue and the development of national cybersecurity strategies by different states.

Cybersecurity has generally been recognised by states as a national security concern in the Asia-Pacific, as confirmed by discussions within the Asia-Pacific Economic Cooperation and the Association of Southeast Asian Nations (Thomas, 2009, pp. 11-14). The establishment mechanisms for cybersecurity cooperation has nonetheless been disjointed because of the differences in the level of resources available to states, as well as the level of public engagement in cyberspace (Heinl, 2013). For instance, Internet perpetration and public awareness regarding cybersecurity are at high levels for technology-oriented states such as Singapore, but the situation is different in Indonesia and Vietnam (Feakin, et al., 2015, p. 11). These discrepancies have generated debates regarding the appropriate national and regional strategies for addressing the increasing number of cyber incidents against several states in the region.

Directly related to the relevance of cybersecurity, is the creation of a national strategy for securing cyberspace. It is problematic that some states have yet to release official cybersecurity strategies considering that the Asia-Pacific is the most active region for cyber conflicts in the world (Valeriano and Maness, 2015, p. 198). In this regard, highly networked small states are arguably the most vulnerable in the region because of their strong dependence on network-technologies but limited capacity and resources to defend their interests against more regional powers.

A cyber strategy is therefore imperative to the survival of small states in the region. The preference to prioritise and develop cybersecurity strategies can be attributed to technology-oriented strategic culture since highly networked states with significant national interests have more incentives to strengthen national cyber strategies to address cyber threats. States that are still struggling to recognise the opportunities facilitated by information and communication technologies may not be confronted with sophisticated cyber threats but they also risk losing considerable economic gains derived from network technology driven industries.

### *Issues and trade-offs of the theory*

NCR is a useful theory for understanding and explaining the foreign policy however, as with all theories, there are issues and trade-offs that need to be addressed when employing it as a theoretical framework (Beach, 2012, pp. 15-16). While there is a substantial amount of published work that considers NCR a progressive theory (Lobell, et al, 2009; Glenn, 2009; Ripsman, et al., 2016), the issues levelled against it are is also significant. This section engages with the debates about the NCR by unpacking the core issues raised against the theory and outlining the trade-offs made in using the theory to explain foreign policy behaviour of small states. Previous work on methodology of scientific research suggests that a theoretical paradigm such as realism is conceptually productive if it meets at least two criteria: coherence and distinctiveness (Lakatos cited in Legro and Moravcsik, 1999, p. 9). The main contention against NCR as a theory within the realist paradigm is that it has flaws in both criteria.

Coherence emphasises the absence of internal logical contradictions that allow the explicit derivation of contradictory conclusions. Whilst theories like NCR advance different supporting assumptions to strengthen its explanatory power, there should be limitations to the extent, which these additional assumptions contradict or deviate from the underlying core assumptions of realism (Legro and Moravcsik, 1999, p. 9). Based on this argument, critics contend that NCR is problematic precisely because it lacks conceptual boundaries and some of its supporting assumptions contradict the basic constructs of realism. Narizny (2017) advances two specific issues that highlight the theory's logical incoherence.

One issue is that there are no explicit conceptual boundaries that define the theory's engagement with domestic politics. This is problematic because the absence of boundaries imply that the theory can accommodate "a wide range of perspectives on social behaviour" without clearly defining which of these behaviours are logically coherent with assumptions of the theory and those which are not (Narizny, 2017, pp. 170, 178). For instance, Narizny (2017, pp. 174-175) contends that the use of strategic culture as a domestic variable to "fill the gap" left by systemic pressures is problematic because culture suggests that states are different thereby contradicting one of the core assumptions of realism: states are undifferentiated by function (James cited in Narizny, 2017, p 160).[8]

Another issue with the theory is that the mechanisms for deciphering whether systemic factors have more influence over domestic or state level factors are imprecise. Since the NCR is not clear about which domestic factors are acceptable, it would be difficult for neoclassical realists "to claim that systemic pressures matter more than domestic factors" (Narizny, 2017, p. 178). On the other hand, if the theory engages more with domestic factors, "it will not be able to sustain its justifying assumption that systemic pressures deserve analytic priority." (Narizny, 2017, p. 178). In this sense, critics such as Narizny (2017) therefore contend that this dilemma creates conceptual confusion that makes it difficult for NCR to facilitate the production of knowledge.

In addressing the issue of incoherence levelled against NCR, the researcher acknowledges that incorporating domestic factors is a problem when applying the theory. The trade-off in the study was to forgo strict adherence to paradigmatic boundaries of realism to justify the interplay between systemic and domestic variables in making sense of cyber capability development in small states. Despite these issues, this thesis mitigates such potential for logical incoherence in two ways. First, the study explicitly justified in the earlier sections of this chapter, why the state level or domestic factor affecting the development

[8] The core assumptions of the realist paradigm are: (1) The most important actors in world politics are territorially organized entities, (2) State behaviour is rational, (3) States seek security and calculate their interests in terms of relative standing within the international system, (4) Anarchy is the ordering principle of international relations, (5) States are undifferentiated by function, and (6) Structure is defined by the distribution of capabilities among states.

of cyber capabilities is strategic culture and not institutions, elite preferences, bureaucratic politics, and other domestic factors postulated in the literature on foreign policy. Designating strategic culture as a state level intervening variable does contradict a core assumptions of realist paradigm, particularly the one which emphasises that states are "functionally undifferentiated" in an anarchic international system (James cited in Narizny, 2017, p. 160). This suggests that states are similar in terms of the functions they perform, the objectives they seek (survival), and the means they utilise to survive in the international system (Waltz, 1979/2010, p. 97). Strategic culture contradicts this assumption because culture draws out beliefs and practices of states that make them dissimilar. The study mitigates this source of incoherence because it explores the technological preferences (i.e. technology-oriented strategic culture) that are common to small states in the region. This analytical focus allows the study to evaluate states based on their relative material capabilities, moderating the differences that culture highlights between states.

Second, the study offered a detailed explanation (Chapter 3) about the contribution of NCR in clarifying the systemic and domestic variables involved in explaining the development of cyber capabilities as a foreign policy instrument. Strategic culture is clearly a secondary condition in the study because strategic beliefs and practices were influenced by the uneven distribution of power in the region (Chapter 5). While Narizny (2017, p. 179) asserts that strategic culture is not an acceptable intervening variable because state preferences "cannot be derived from the survival motive", this study demonstrated that this assertion is flawed. The material constraints imposed on small states due to limited natural resources and unfavourable geographic location influenced the strategic preferences of New Zealand, Singapore, and Brunei. In this sense, the survival of these states is predicated on their ability to exploit networked technologies strategically to adapt to the changing geopolitical environment.

The other criteria, distinctiveness, highlights that the assumptions of a theory should differentiate it from other theoretical alternatives (Legro and Moravcsik, 1999, p. 10). A key strength of NCR is designed to accommodate domestic factors into its explanatory framework but this integration should not undermine the distinctiveness of the theory. Critics dismiss the potency of NCR because it is "indistinguishable from nonrealist theories about domestic institutions, ideas, and interest" (Legro and Moravcsik, 1999, p. 28). International Relations scholars point out two main issues that underscore the theory's lack of distinction.

The first, raised by Legro and Moravcsik (1999, p. 28), is that NCR suffers from "theoretical indeterminancy and a reliance on exogenous variation in state preferences." In this sense, "theoretical indeterminancy" refers to the theoretical framework's inability to clarify the weight or significance of material and ideational variables that are integrated within a coherent explanatory framework. On the other hand, the reliance on a variation of "exogenous" or external domestic variables makes it difficult to differentiate the theory from liberal and epistemic paradigms that also focus on exogenous variation in state preferences but differ in how these preferences are formed and expressed. Liberal theories provide that state preferences are formed by individuals and groups that influence representative institutions and practices to translate their interests into state policy (Moravcsik, 1997, p. 218). On the other hand, epistemic theories hold that state preferences are formed through collective beliefs and ideas of an epistemic community or "a network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area" (Haas, 1992, p. 3). Moreover, Haas (1992, pp. 2-3) contends that diffusion of beliefs and ideas "can lead to new patterns of behavior and prove to be an important determinant of international policy coordination." Deprived of clear distinctions between these alternative theories, the advantages offered by NCR as a foreign policy theory are diminished and the theory ceases to be conceptually progressive.

A second issue articulated by Narizny (2017), is that NCR is not distinctive enough to be considered as part of the realist paradigm. He asserts that the realist theories such as offensive, defensive and hegemonic are distinctively realist because they are anchored on the core assumptions of the paradigm. NCR is problematic, Narizny (2017) points out, because it incorporates variables that contradict the core assumptions of realism thereby creating confusion regarding the potency and veracity of the theory. For example, in reviewing the works of NCR scholars such as Brawley (2010), Dueck (2006), Schweller (2006) and Layne (2006), Narizny (2017, pp. 171-177) claims: "none of the four authors holds the same view of neoclassical realism." The variety of interpretations offered by

International Relations scholars suggests indistinctiveness of the theory because is no consensus regarding the defining features of the theory as well as how it is located within the realist paradigm. In concluding, he suggests that NCR should not be part of the realist paradigm and is better off as part of other paradigms such as "realist constructivism" or "none at all, per "analytic eclecticism." (Narizny, 2017, p. 188).

NCR is not as distinctive as other theories within the realist paradigm. The trade-off in the study was to accept "minimal realism" as a guiding principle to explore a more integrated explanatory framework to explain the development of cyber capabilities in small states. "Minimal realists seek to define a distinct and coherent realist paradigm with reference to a set of assumptions that are less restrictive" than the core assumptions of realism (Legro and Moravcsik, 1999, p. 19). Consistent with this principle, the study is primarily anchored on realism because it while is does not strictly adhere to the "undifferentiated function" of states; it still follows the other five paradigmatic assumptions. In this sense, the study accentuates the role of anarchy in shaping the online and offline interactions of states within the region (Chapter 1). It highlights that states or "territorially organised entities" are the most important actors in the international system (Chapter 1). It argues that small states are rational because they develop cyber capabilities in response to geopolitical tension in the region (Chapter 4). It advances that small states develop cyber strategies that are consistent with their relative standing within the international system (Chapter 4). Lastly, the study suggests that the uneven distribution of capabilities influences the structure or hierarchy of cyber powers in the region (Chapter 1 and 4).

## Conclusion

Theories are instrumental in developing a more systematic and profound understanding of state interactions in cyberspace. This chapter introduced a theoretical framework that combines neoclassical realism and strategic culture to explain why small states develop cyber capabilities and how these capabilities are utilised as foreign policy instruments by small. Before presenting the framework, the chapter clarified key conceptual issues such as the levels of analysis involved in the study and expounded on the idea of cyber capabilities as foreign policy instruments of states. Since information and communications technologies pervade all aspects of state and society, the study considers two levels of analysis:

system and state. Moreover, the distinct characteristics of computer networks also make cyber capabilities useful instruments for small states to advance foreign policy interests.

The chapter then discussed the main analytical themes and the alternative theoretical paradigms. Following the core assumptions of realism, the study focuses on anarchy, the relative distribution of power, and interaction between systemic and domestic factors as the major analytical themes. Contending theoretical paradigms such as liberalism, constructivism, and technological determinism were considered as alternative frameworks however, neoclassical realism was recognised as the most appropriate because it provides a more inclusive and systematic framework that strengthens argument of the study.

Neoclassical realism was operationalised in the chapter by defining the relevant variables, observable implications, and the measurements to implement the study. Consistent with the research design, the primary (distribution of power) and secondary (strategic culture) variables were treated as necessary conditions for the development of cyber capabilities. The framework is applied through a qualitative assessment of the observable implications implemented through the specific measurements identified. The next chapter analyses the distribution of power as the principal condition that affects the development of cyber capabilities. In exploring this condition, Chapter 4 considers four main analytical themes: the geopolitical constraints in the region; the responses of small states to cyber conflict; the contribution of computer network operations in conventional military operations; and the value of cyber power in the strategies of selected states.

# Chapter 4
## Distribution of Power and Cyber Capability Development

Cyber capabilities have emerged as fundamental instruments for states to advance their strategic interests in an uncertain security environment. States engage in computer network attacks to signal a calibrated response to prevailing political and territorial disputes between neighbouring states in the Asia-Pacific Region. Within the range of foreign policy options, cyber operations are emerging to be strategic instruments since they are useful in "influencing the space between overt diplomacy and overt war" because these capabilities can disrupt or even destroy information critical to states' national security without causing physical damage or harm (Brantly, 2014, p. 465). Indeed, these network intrusions have been employed by states to convey their foreign policy preferences without significantly damaging diplomatic relations and intensifying instability in the region (Libicki, 2009, pp. 28-29). Following these conditions, states can best exploit the advantages of cyber capabilities when strategically utilised to support existing foreign policy instruments such as diplomacy, economic transactions, and military force.

This chapter contends that the relative distribution of power in the Asia-Pacific is a necessary condition for the development of cyber capabilities in small states. It advances the argument by drawing on the theoretical framework developed in Chapter 3, in which the unequal distribution of power is treated as a principal condition necessary for small states to invest in cyber capabilities. Since the study aims to develop limited generalisations and not causal inferences about the foreign policy behaviour of small states, the method of structured and focused comparison advocated by George and Bennett (2005) will be applied in the next three chapters. This method enables the researcher to test the strength of the theoretical framework in explaining the development of cyber capabilities in small states in the region.

In applying this method, the subsequent sections of this chapter are focused on a set of themes constructed from the theoretical framework and concepts presented in Chapter 2. These themes are structured around a set of common questions that explore the relative distribution of power in the region:

1. How do small states respond to cyber conflict in the Asia-Pacific Region?
2. How do cyber capabilities relate to conventional military capabilities of small states?
3. What is the contribution of cyber power to the foreign policy strategies of small states?

The rest of this section explores the main sources of cyber conflict and how these related to the relative distribution of power in the region. The second section addresses the first question by investigating how the selected states have responded to cyber conflict in the context of their limited capabilities and resources relative to powerful states in the region. The third section examines the contribution of computer network operations in conventional military operations and how these capabilities support the respective strategies of the selected states. The fourth establishes the connection between cyber capabilities and state power, particularly the value of cyber power in the strategies of selected states. The last section summarises the main themes of the chapter and links the findings with the overall argument of the study.

### *Sources of cyber conflict in the region*

Cyber conflicts in the Asia-Pacific are driven by the prevailing geopolitical conflicts that have influenced state behaviour in cyberspace (Asia: The Cyber Security Battleground, 2013; Maurer, 2015). For instance, territorial disputes are a source conflict that has instigated cyber intrusions in the region (Boland, et al. 2015). Indeed, studies on interstate conflict suggest that territorial disputes are more war prone than other sources of conflict because "human territoriality encourages the establishment of borders through aggressive displays" (Valeriano and Vasquez 2010, p. 3). Small states that are involved in these territorial disputes are typically disadvantaged because of their limited resources and military capabilities to defend their interests against more powerful states. In this context, powerful states such a China utilise computer network operations as a less intrusive strategic to signal discontent against the actions of weaker states that are directly or indirectly involved in geopolitical conflict in the region such as such as Singapore, Vietnam, and Taiwan (Segal, 2017; Lewis, 2018).

The idea of signalling intentions is derived from the literature on covert communication that explains how states bargain for their foreign policy interests by employing covert signalling (Carson and Yarhi-Milo, 2017). Research in this area reveal that states secretly convey their intentions to adversaries through "costly signals" or statements and actions "designed to persuade the other side that one is trustworthy by virtue of the fact that they are so costly that one would hesitate to send them if one were untrustworthy" (Kydd, 2000, p. 326).

The notion of covert signalling was first introduced by Schelling (1960/1981) and George (1983). Schelling's bargaining framework presented two key concepts: "focal points" and "salient thresholds" (Schelling, 1960/1981, 1966/2008). Schelling discussed that "focal points" are patterns of behaviour that are mutually recognised by interacting states (Schelling, 1960/1981, pp. 57-58) while "salient thresholds" refer to distinctive restraints that are recognised by both sides to "indicate what is within bounds and what is out of bounds" (Schelling, 1966/2008, pp. 135-141). George (1983) meanwhile, used these concepts to explain the crisis behaviour between great powers, which included covert action. He argued that the U.S. and Soviet Union created "an ad hoc set of ground rules" that guided their intervention in external conflicts (George cited in Carson and Yarhi-Milo, 2017, p. 132).

Exploiting cyberspace for covert signalling has strong potential particularly because of its conduciveness to secrecy and stealth (Poznansky and Perkosky, 2018). Indeed, powerful states such as China, Russia, the U.S., and have already employed sophisticated cyber operations to discreetly convey their foreign policy preferences during the past decade. It is unclear however, how small states with cyber capabilities can take advantage of covert signalling as a bargaining mechanism to advance their foreign policy interests. This dilemma will be discussed in more detail in the subsequent parts of this study.

Aside from territorial disputes, the other two main sources of cyber conflicts are great power rivalry and historical animosities because these factors contribute to the procurement and upgrade of conventional military capabilities (Tan, 2014, pp. 105-141). The great power rivalry between China and the U.S. is a dominant factor that continues to affect the distribution of power in the region. The extension of great power competition into cyberspace has escalated since the start of the twenty-first century thereby increasing uncertainty regarding state interactions in cyberspace (Domingo 2016). While both powers have invested extensively in conventional military capabilities, they have also militarised cyberspace by developing cyber commands, creating doctrines for cyber operations, and rationalising policies that enable military responses to cyber conflict (Manson, 2011). More importantly, these states already have high levels of expertise in employing complex computer network operations in support of their respective foreign policy objectives, some of which relate to tensions in the Asia-Pacific (Valeriano and Maness, 2015, p. 88).

The rivalry between two powers may not directly initiate cyber conflict but it heightens the uncertainty in the region through the militarisation of cyberspace. The militarisation of cyberspace by great powers contributes to uncertainty because there is insufficient knowledge about cyber operations to determine the relative capabilities of each state (Liff, 2012, p. 402). While China and the U.S. have demonstrated their capabilities through several cyber incidents, there is no conclusive assessment regarding the capabilities of these states. The ambiguity surrounding the impact of cyber weapons has influenced other states' responses to uncertainty by hardening network defences and enhancing situational awareness.

The choice to disclose or conceal the existence of cyber capabilities is deliberate strategy for great powers because ambiguity provides them with more bargaining options that can be expressed through covert signalling through as cyber operations. The dynamics behind covert communications is that enduring rivals such as China and U.S. have developed a "basic interpretative framework" that they use to communication during crisis situations (Carson and Yarhi-Milo, 2017, pp. 125-126). A cyber operation is one instrument that operationalises this framework. This secret cooperation is developed through years of extensive intelligence activities that aim to understand the intentions and capabilities of each other. This covert bargaining provides both states with more options to resolve specific foreign policy issues because it limits the audience costs that can damage state leadership and/or relations with other states during crisis situations such a collision between military surveillance aircraft or a network security breach that compromises government databases.

A third source of cyber conflict is the historical animosities between rival states in the region. Hostilities that involve religion and ethnicity have generated insecurity between rivals and compelled the steady investment of conventional military capabilities of certain states in the region. Some notable examples include conflicts between North and South Korea, China and Taiwan, India and Pakistan, and Singapore and Malaysia. These states need to maintain capable and effective military forces to project a strong strategic posture and ensure a credible military response to adversaries (Tan, 2014, pp. 113-124). Modern military platforms such as the fighter jets and subsystems for air-defence however, all run on information and communication technologies and therefore require cyber capabilities to counteract intrusions and prevent systems from being compromised. In this sense, computer network operations have become necessary tools to protect military forces from cyber threats. While enduring animosities between states do not directly contribute to cyber conflict, these conflicts encourage the development of conventional military capabilities that subsequently require cyber capabilities for network defence.

The predominance of cyber conflict and its relation to existing rivalries and dispute has created a strategic dilemma for states because a definitive and clear response to increasingly sophisticated cyber intrusions has yet to be determined by the international community. This "cybersecurity dilemma" is conceptualised as the tendency of states to threaten other states' security by intruding into strategically significant networks to assure their own cybersecurity, thereby risking escalation and undermining stability (Buchanan, 2016, p. 3). The core of the dilemma is the idea that computer network intrusions are conducted for both offensive and defensive purposes, and states are not certain which of these objectives are in play. Since it is difficult for states to determine the intentions and capabilities of other states in cyberspace, uncertainty constrains the behaviour of states in the region.

Network intrusions employed by powerful states are prominent examples of this dilemma; recent reports suggest that cyber operations have utilised to exploit the communications and computer networks of both adversaries and allies. China for instance, contributes to the cybersecurity dilemma because its computer network intrusions gathered massive amounts of classified information and intellectual property from states regardless if these are important trading partners like South Korea, benign neighbours like Malaysia or small states such as Brunei and Singapore (Geers, et al., 2014; Boland, et al., 2015). On the other hand, the U.S. contributes to uncertainty in the region through its network intrusions against different allies in Europe, Latin America, and Asia. (Easley, 2014; Walsh and Miller, 2016). These network infiltrations function as "due diligence" to verify that the intentions and actions of allies are consistent with the national interests of the U.S. (Easley, 2014).

*Relative distribution of power*

The conditions generated by the different sources of conflicts region has contributed to the sustained build-up of conventional military weapons, which in turn necessitates cyber capabilities to defend military and government networks. The expansion of military capabilities in the region however has produced an imbalanced distribution of power that favours great powers and places less powerful states at a disadvantage in terms of material resources and the capacity to mobilise these resources. The relative power distribution in the region is therefore a decisive factor that affects the foreign and security strategies of less powerful states. Building on this logic, the relative power distribution between states can be treated as a dominant condition for weaker states to develop cyber capabilities. There are three reasons that support this assertion.

First, the relative distribution of power solidifies the strategic advantages afforded to the "first movers" or states that first introduced and adopted the use of cyber capabilities in the region. Since China and the U.S. were the first to use of such computer network operations in the region, these states have already refined the use of computer network operations to achieve their respective foreign policy objectives (Healey, 2013; Valeriano and Maness, 2014). In fact, these states have a stronger incentive for employing computer network operations since "first movers" typically enjoy a temporary monopoly over new military innovations considering that less powerful states do not always have the financial resources and organisational capital to pursue new military technology (Horowitz, 2010, p. 16). In addition, the rivalry between "first movers" further complicates the power distribution since both powers have expressed the intention to extend their existing military competition in cyberspace (Domingo, 2016). As discussed in the previous chapter, the rivalry amplifies the uncertainty in the region, which affects the strategic posture of weaker states in the region.

Second, the relative power distribution in the region affects the foreign and security policies of medium and small states due to the power shift in favour of China. China's military capabilities are unrivalled the region and its actions in the digital domain reflect its intention to maintain regional dominance as well. In consolidating its power, China has gained strategic advantages from exploiting other states' computer networks to achieve its foreign policy objectives. China's military cyber operations are extensive and well documented. The People's Liberation Army (PLA) has systematically targeted multiple actors and managed to obtain a substantial amount of state secrets by infiltrating computer networks of both adversaries and allies with minimal consequences (Stokes, 2015).

Whereas intelligence gathering through cyberspace is different from network attacks that deny or destroy information, these intrusions threaten the security of other states for at least two reasons. The first is these can enable directed and powerful cyber attacks by China because detailed targeting information have been collected and processed (Lindsay, 2015, p. 33). The second is that these intrusions facilitate further cyber operations because Chinese attackers can "piggyback off" an "already-existing presence" inside computer networks of other states (Buchanan, 2016, pp. 81-84). As a result, states in the region have become increasingly insecure about China's cyber espionage operations to the extent that some national cyber strategies (e.g. Australia, New Zealand, Singapore, and South Korea) have prioritised countermeasures to mitigate the threat of cyber espionage.

Third, the relative power distribution has forced small states to rethink strategic options besides aligning with powerful states. Studies on small state foreign policy suggest that these states align themselves with great powers to increase their chances of survival in an anarchic international system (Waltz, 1979/2010). Foreign policy alignment is a predominant occurrence in the region given the enduring power struggle between the China and U.S.  To manage this great power competition, small states have pursued in three general alignment strategies in the region: balancing, bandwagoning and hedging (Roy, 2005; Cooper and Lim, 2015). Although foreign policy alignment is instrumental to the survival of small states, it is unlikely that balancing or bandwagoning will have any consequential effect on the cybersecurity of small states. There are two reasons that explain this contention.

The first reason is balancing and bandwagoning with great powers involves enhanced cooperation and information exchanges regarding military capabilities. These strategies require small states to increase dependence on great powers that requires developing interoperability between military forces and sharing access to intelligence, surveillance, and reconnaissance (ISR) systems. These measures are cybersecurity challenges because they can expose military forces to network vulnerabilities such as the "disruption, corruption, and theft of data" (Hura, et al. 2000, p. 11). Since great powers have more capacity and resources to operate in cyberspace, they have fewer incentives to disclose the scope and range of their capabilities.

International cooperation is an essential component of national cyber strategies but there are limits to what small states can gain from great powers in the area of cybersecurity. While less powerful states have more to gain than lose from information sharing about cyber capabilities, the advantages afforded by cyber weapons are temporary because unlike conventional military weapons, these are "highly transitory" or their "ability and effectiveness to cause harm declines relatively quickly" (Smeets, 2017, p. 7). For instance, once a zero-day vulnerability[9] is exploited, it takes an average of 312 days before patches are installed and vulnerabilities are closed (Bigle and Dumitras, 2012). In this sense, states engaged in alliances and strategic partnerships will be cautious of sharing all information regarding cyber capabilities if they intend to preserve the potency of their cyber weapons.

Another example that relates this argument is the relationship between less powerful states and the United States within the Five Eyes intelligence network. Previous research on this topic suggest that although Australia and New Zealand are contributors to the network, they are able to exercise some degree of autonomy and do not always rely on the network to enhance their intelligence collection through cyberspace (Anthony Smith, personal communication, June 17, 2016; O'Neil, 2017). Moreover, sharing information becomes a restraint rather than an advantage particularly when powerful states with extensive resources have divergent foreign policy objectives with small states (Lefebvre, 2003, pp. 534-535). In this context, cooperation in the area of cybersecurity is not always helpful because there are technical and political barriers that prevent less powerful states from utilising cyber capabilities strategically.

[9] The term refers to a security weakness or flaw in software that is "unknown to the software maker or to antivirus vendors" (Zetter, 2014).

The second is that cyber weapons do not deliver the same strategic effect as conventional military weapons hence the security guarantees provided by alliances and strategic partnerships will have a reduced effect when tackling cyber conflict. Since cyber weapons do not inflict physical harm or damage, cyber incidents have not prompted a conventional military response from states. A prominent case that supports this point is the distributed denial of service attacks (DDoS) against Estonia in 2007. Despite the extensive scope of the DDoS attacks, Estonia was unable to convince the NATO to respond to Russian-based computer network attacks using military force since NATO did not consider the cyber incident as a case of clear military action (Crandall, 2014, p. 36). While NATO has developed a more aggressive response to cyber intrusions by releasing a Cyber Defence Pledge and including cyber defence as a principal task of collective defence: the official response to computer network attacks still remains restrained: "A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis" (North Atlantic Treaty Organization [NATO], 2014, 2016).

The limitations of addressing cyber threats through alignment with great powers has influenced some small states to independently generate the capacity to defend their national interests in cyberspace. Developing cyber capabilities is consistent with the strategy of hedging because it necessitates self-reliance to avoid depending on great powers in the region. Hedging like balancing and bandwagoning, is foreign policy strategy that small states employ to enable them to advance their foreign policy interests in the anarchic international system. The key difference with hedging is that it involves maintaining ambiguity regarding a small state's alignment with great powers while balancing and bandwagoning necessitates clear intentions about the alignment of a small state with great powers (Lim and Cooper, 2015, pp. 696-698). Since hedging involves uncertainty in foreign policy alignment, building robust cyber capabilities can contribute to strengthening the autonomy of small states in terms of foreign policy since they will minimise their dependence on powerful states particularly in the area of national security.

## Cyber conflict and strategies of small states

The emergence of network technologies became an opportunity for states to transform cyberspace into an environment for pursuing interstate rivalries and political disputes. States use cyber capabilities as an alternative tool to mitigate the uncertainty and emerging threats generated by uneven distribution of military capabilities and resources in the region. Developing strategies to counter cyber threats in a complex security environment is more problematic for small states given their limited capabilities and resources to respond to cyber conflicts (Burton, 2013; Heng, 2013). This section compares the cyber strategies of New Zealand, Singapore, and Brunei with the objective of understanding how these states respond to cyber conflict. In analysing cyber strategies, the section draws on the work of Klimburg, et al. (2012) which identifies objectives or "mandates" of national cybersecurity strategies based on five themes: military, intelligence, cybercrime, critical infrastructure protection, and diplomacy. These mandates will be used as categories to provide a more systematic comparison of the three cases.

### *Military*

The role of the military in the cybersecurity strategies of New Zealand, Singapore and Brunei is predominantly focused on protecting military computers and networks against cyber threats but the extent to which the military is involved varies across the three states. The New Zealand Defence Force (NDZF) was traditionally configured to be more assertive by supporting powerful allies and contributing to collective security arrangements. This orientation however, changed to non-conventional military operations such as peacekeeping operations and disaster relief due to the anti-militaristic ideology espoused by the Labour Government when it assumed power in 1984 (McGraw, 2008, pp. 23-30). Labour's view was influenced by the low threat environment, geographic isolation, and limited resources for military power projection that defined New Zealand's strategic posture.

This benign strategic environment is no longer valid in the twenty-first century with the advent of computer network attacks that are linked to geopolitical tensions but are not constrained by territorial boundaries (Singer and Friedman, 2014, pp. 68-69). Moreover, the militarisation of cyberspace by powerful states and the emergence of cyber conflict linked to geopolitical tensions in the region have shaped a complex strategic environment from which New Zealand is no longer insulated (New Zealand Ministry of Defence, 2016, p. 29).

These conditions have compelled New Zealand to adjust to the relative distribution of new military capabilities across the region by initiating the development of a new cyber support capability "to improve protection for Defence Force networks and provide dedicated support for deployed operations" (New Zealand Ministry of Defence, 2016, p. 51). The NZDF is still at the early stages of cyber capability development and the main priority is to delineate the appropriate organisational and personnel arrangements required to support the new military capabilities. In essence, the New Zealand Government considers the development of cyber capabilities as a fundamental upgrade to existing conventional military capabilities in preparation for sophisticated and persistent cyber incidents that may arise from uncertainty and conflict in the Asia-Pacific Region (New Zealand Ministry of Defence, 2018, pp. 16-22).

In contrast, the SAF was formed during a tumultuous period in Singapore's history, considering its involvement in the *Konfrontasi* between Indonesia and Malaysia that escalated in 1963. This instability was further exacerbated when the Singapore was separated from Malaysia in 1965, compelling its leaders to establish an independent and sovereign state (Huxley, 2004, p. 185). These historical circumstances and the state's inherent limitations in natural resources, population, political influence, and size relative to other states in the region, have shaped its strategic preference for investing in advance technology as well as its drive to develop one of the most capable military forces in the region. Maintaining an effective and highly capable military force is the cornerstone of Singapore's strategy given its lack of strategic depth and military personnel (Huxley, 2004, pp. 185-186).

While both New Zealand and Singapore recognise network defence as a key motivation for developing military cyber capabilities, Singapore has more strategic interests at stake given the superior status of its military force and its active engagement with neighbouring states in the region. In this sense, preserving the SAF's technological edge over other military forces requires the development of cyber capabilities to protect advanced military platforms and subsystems that are enabled by computers and networks. Moreover, the build-up of conventional military capabilities in the region provides a rationale for Singapore to revaluate its capabilities to confirm its "one generation" lead ahead of the other military forces in the region (Bernard Loo, personal communication, July 27, 2016).

Despite the SAF's clear inclination towards technological superiority, there are very few details regarding its cyber operations. One initiative is the institution of a Cyber Defence Operations Hub in 2013 that signifies the SAF's intention to improve its threat detection and analysis and reinforce network defence against emerging cyber threats (Phneah, 2013; Singapore Ministry of Defence, 2017). A more recent initiative is the development of the Cyber Defence Organisation that is tasked to "oversee policies, capability development and implementation to monitor and defend" the computer networks of the Ministry of Defence and the SAF from cyber threats. The impetus for this new military organisation is the "significant growth in the risk of cyber threats against countries, in particular, the increase in threats towards the military and the networks of defence industry and military related organisations" (Singapore Ministry of Defence, 2017). Given these initiatives, the SAF's primary purpose in developing cyber capabilities has been to support its conventional military capabilities through cyber defence (He, 2015, p. 66).

Analogous to the SAF's experience, the Royal Brunei Armed Forces (RBAF) was also formed during a tumultuous period in Brunei's history, given its hostile interaction with Indonesia and Malaysia during the 1960s and 1970s. Although these historical experiences impressed a sense of insecurity and vulnerability in the state's strategic posture, Brunei has benefitted from a benign external security environment and has not been threatened by any external power since its independence from the UK in 1984 (Cheng-Chwee and Welsh, 2005, p. 61). Following this favourable external environment, Brunei has realigned its strategic posture by maintaining a very small military force but unlike New Zealand and Singapore, it does not develop a strong citizen reserved force to support its military operations due to its limited population to recruit from and reliance on external security assistance from the UK (Kershaw, 2011, pp. 113-114; Criossant and Lorenz, 2018, pp. 26-27).

Brunei however is aware that its limited involvement in geopolitical tensions and military conflicts does not guarantee fewer incidents of cyber conflicts given that computer network attacks do not trigger the same response as conventional military attacks. The Brunei Ministry of Defence has therefore identified computer network attacks as an important concern: "Threats to information systems can undermine competitive advantage and reveal sensitive national information" (Brunei Ministry of Defence, 2011, p. 7). Brunei recognises the significance of ICTs in military affairs however, it is not yet to develop a dedicated national cybersecurity strategy like New Zealand or establish a cyber command like Singapore.

Indeed, technological advancement within Brunei has been gradual considering that the state "realised the importance of Science & Technology (S&T) for national security" in 2011 and released the *Defence Science and Technology Policy Framework* several years after in 2016 (Brunei Ministry of Defence, 2011, 2016). While this framework will take several years to implement, it is crucial because it defines the foundations and policy direction of the military in exploiting ICTs as force multipliers as well as confirming the state's commitment to modernising its military force (Brunei Ministry of Defence, 2016). The absence of an explicit strategy for cyberspace can be attributed to the state's general reluctance to leverage the advantages afforded by ICTs because of its potential to facilitate new ideas that can contradict the beliefs and practices espoused by its national ideology of *Melayu Islam Beraja* (MIB) or Malay Islamic Monarchy (Besar, 2015). Chapter 5 presents a more comprehensive discussion about Brunei's national ideology.

### *Intelligence*

The role of intelligence agencies in addressing cyber issues in Brunei, New Zealand and Singapore is mainly focused on information collection and analysis however an in-depth account of these activities is not possible at this time. New Zealand's Government Communications and Security Bureau (GCSB) is the lead intelligence organisation tasked to identify and respond to highly evolved cyber threats relating to geopolitical tension in the region. The main contribution of GCSB in the Government's cybersecurity strategy is its expertise in intelligence and cybersecurity. More specifically, the GCSB is responsible for gathering and analysing intelligence regarding cyber threats against communication systems and information infrastructure and advises government leaders about the countermeasures necessary to address these threats (Government Communications Security Bureau [GCSB], 2014, pp. 6-7).

Another contribution is the GCSB's intelligence cooperation with Australia, Canada, U.K., and U.S. or the Five Eyes (FVEY) intelligence network. Whilst the primary purpose of the network is to share intelligence collected through cyberspace, it forces New Zealand to ensure that the GCSB is aligned with allied agencies by maintaining robust information assurance practices as well as the necessary capabilities and resources for computer network exploitation against adversaries (Burton, 2013). These initiatives suggest that New Zealand's interest to develop and maintain capabilities for cyber espionage is in line with its strategy to cope with the impact of the uneven power distribution between states in the region by using the intelligence network to identify and mitigate potential threats (Anthony Smith, personal communication, June 17, 2016).

The Security and Intelligence Division (SID) of Singapore's Ministry of Defence is the primary organisation that collects foreign intelligence, particularly human and signals intelligence against adversaries (Huxley, 2000, pp. 89-90). In contrast to New Zealand, the role of intelligence organisations in Singapore's cybersecurity strategy is not clearly defined in any official public document. Its responsibility for signals intelligence collection however, suggests that it is capable of computer network exploitation considering the SAF's strong reputation of deploying cutting-edge military technology (Matthews and Yan, 2007; Huang, 2009; Ng, 2017).

A significant but unacknowledged aspect of Singapore intelligence operations has been its cooperation with the FVEY intelligence network. While not an official member of the network like New Zealand, the state has been identified as a partner in monitoring telecommunications around the world by tapping high-speed fibre optic cables, enabling the most powerful intelligence network to expedite their mass surveillance activities (Dorling, 2013; Alan Chong, personal communication, July 7, 2016). This cooperation is driven by Singapore's interests to preserve the balance of power by supporting U.S. efforts to counter China's military aggression in different strategic environments while developing deeper defence ties with China (Tan, 2012; Emmers, 2015). Following these actions, Singapore's involvement in computer network exploitations indicates that its strategic posture is influenced by the relative distribution of power in the region. The state's support of the FVEY intelligence network while asserting its independence through non-alignment with any great power confirms Singapore's intention of utilising cyber capabilities to independently defend its national interests in cyberspace as well as reinforce its response to computer network attacks by adversaries.

The Internal Security Department (ISD) is Brunei's main intelligence organisation that is attached to the Prime Minister's Office. Similar to the Singapore case, the ISD's role in Brunei's national cybersecurity efforts is not clearly documented in any official public document however, ISD's mandate of monitoring incidents of subversion, espionage, and sabotage makes it a key organisation in Brunei's move towards building a digital government (Brunei Prime Minister's Office [BPMO], 2012). For instance, the ISD was in charge of deporting four Indonesian nationals for obtaining and spreading propaganda materials related to the Islamic State through the Internet and more recently detained a local for engaging in self-radicalisation through the Internet (Brunei Information Department, 2017; Hayat, 2018). In this context, the efforts of the ISD is centred on monitoring internal or domestic security threats with the objective of defending the state's national ideology and maintaining the political; status quo.

Since Brunei has yet to develop a specific cyber strategy like New Zealand and Singapore have, the ISD's primary mission of providing "early warning to the government on any imminent threats" is crucial in navigating through a regional strategic environment shaped by significant power discrepancies between states (BPMO, 2012). Indeed, the Brunei National Energy Research Institute, which is also managed by the Prime Miniter's Office, published a study suggesting that Brunei's power plants are vulnerable to disruption and damage in several areas including "generation system, transmission system, distribution system" among others (Chaudhary, et al., 2015, p. 6). The report acknowledges the vulnerability of these power plants from malicious software such as Sandworm and Stuxnet that are reportedly state-sponsored and specifically target supervisory control and data acquisition (SCADA) systems in industrial systems (Chaudhary, et al., 2015, pp. 10-11). The preference for coordinating both technical expertise and intelligence assessment under one office links to Brunei's conditioned strategic culture that favours a centralised governance structure that enables the Sultan to supervise practically most if not all the crucial issues that relate to foreign and security policy.

### *Cybercrime*

Counteracting cybercrimes has been a core focus of the cybersecurity efforts of New Zealand, Singapore and Brunei. Even though cybercrimes are transnational in nature, anti-crime initiatives of the selected states have been mainly focused on domestic countermeasures such as improving operational response capabilities to cyber incidents, developing public-private partnerships to address cybercrimes, and promoting cybersecurity education and training. From a strategic perspective however, efforts of the respective governments have focused more on maintaining cybersecurity legislation in line with international norms and agreements on cybercrime because of the security issues associated with cybersecurity cooperation.

A fundamental challenge that relates to the power imbalance in the region is the uncertainty regarding the capabilities and strategies of states for cyber operations including cybercrime. This condition is a strong incentive for states to be less transparent about their cyber capabilities and be suspicious regarding the capabilities and intentions of other states in the region. While international institutions such as the International Police (INTERPOL) and Asia Pacific Computer Emergency Response Team (APCERT) are mandated to improve cooperation in the area of cybercrime, there are still more incentives for states to remain very selective about what they disclose regarding their cyber capabilities.

A key factor that affects cooperation is the clashing views of states regarding the governance of cyberspace. For instance, China is less cooperative in sharing information with states in the region consistent with its idea of cyber sovereignty (Hakmeh, 2017; Heinl, 2018). Another example is the refusal of powerful states China and India to ratify the Budapest Convention on Cybercrime, the only legal instrument designed to facilitate international cooperation to counter cybercrime. The basis of their rejection is either they were not involved in the drafting process or because it violates on their sovereignty (Grisby, 2014; Hakmeh, 2017).

New Zealand cybercrime efforts are well developed. The state enforces a number of laws that deal with cybercrime, a *National Plan to Address Cybercrime (2015),* technical measures implement the national plan (e.g. computer emergency response team), and strategic public-private collaboration on cybercrime (National Cyber Policy Office [NCPO], 2015c, p. 8; International Telecommunications Union [ITU], 2014, p. 348).[10] Singapore's cybercrime

[10] Directly relevant cybersecurity laws in New Zealand include the *New Zealand Security Intelligence Service Act 1969*, the *Privacy Act 1993,* the *Electronic Transaction Act 2002,* the *Government Communications Security Bureau Act 2003,* the *Unsolicited Electronic Messages Act 2007,* the *Electronic*

initiatives are in the same direction as New Zealand's since it has laws that address computer-related crime, a *National Cybercrime Action Plan (2016)*, technical measures implement the national plan, and increased collaboration between public and private organisations.[11] Brunei meanwhile has the laws and the technical measures to tackle cybercrimes but lacks two key elements in comparison with New Zealand and Singapore. Firstly, Brunei has no clear implementing plan for countering computer crimes. This make it more difficult for Brunei to determine if its cybersecurity initiatives are effective and more importantly whether it is actually progressing towards its objective of providing "a resilient and trusted digital platform that maximises the full potential of the digital space" (BPMO, 2015, p. 8). Secondly, although there are established links between the public and private sectors in the area of cybersecurity, the government dictates the direction of the collaboration (Feakin, et al., 2016, pp. 25-26).[12] Strong government regulation and intervention on cybersecurity issues is a challenge for Brunei because it limits innovation and weakens accountability regarding government operations in cyberspace. These institutional arrangements can be attributed to standard practice in Brunei that prescribes government intervention in all critical aspects of the states such as the use and management of ICTs.

While these states seem to have domestic measures in place, their proposed strategic, externally oriented initiatives are still underdeveloped. For instance, both New Zealand and Singapore identify building international networks as a key strategy to address cybercrime but these states have yet to accede to the Budapest Convention on Cybercrime because of several critical issues such as international jurisdiction and consistency with domestic laws (Weber, 2003; Thomas, 2009). Another specified strategy is to work with the international institutions such as the ASEAN and the Asia-Pacific Economic

*Identity Verification Act 2012, The Telecommunications (Interception Capability and Security) Act 2013,* and the *Harmful Digital Communications Act 2015* (ITU, 2014, p. 348).

[11] The *Computer Misuse and Cybersecurity Act 2013* is the primary law that focuses on cybercrimes but the Singapore Government has released a draft of the *Cybersecurity Act 2017* for public consultation. This proposed law aims to empower the Cyber Security Agency "with the necessary powers to effectively address increasingly sophisticated threats to national cybersecurity." (Cyber Security Agency, 2016, p. 18).

[12] Directly relevant cybersecurity laws in Brunei include the *Official Secrets Act 1998, the Computer Misuse Act 2007*, the *Electronic Transactions Act,* the *Anti-Terrorism (Financial and Other Measures) Act,* the *Broadcasting Act - Internet Code of Practice, and* the *Copyright Order 1999* (ITU, 2014, p. 106).

Cooperation (APEC). This initiative however, has proven to be weak for two reasons.

First, the unequal distribution of cyber capabilities among states in the region is a disincentive for states to cooperate and share resources to mitigate cybercrimes. Similar to the argument on cyber weapons, there are limits to what states are willing disclose about their expertise and resources regarding network vulnerabilities and computer forensics for example, even if these are essential in investigating computer-related crime (Inserra and Rosenzweig, 2014; Brewster, 2014). Whereas small states such as Singapore and New Zealand are actively engaged in cybersecurity CBMs in the region, cyber powers such as China, Russia and the U.S. are more cautious in cooperating with each other in the area of cybersecurity mainly because of their fundamental disagreements about cyberspace governance and previous experiences with cyber intrusions (Grisby, 2017; Segal, 2017b; Goldsmith and Williams, 2017).

Second, regional institutions are incapable of coordinating regional efforts to address the prevalence of cybercrimes. One challenge is that international institutions still lack a coherent policy approach to synchronise the efforts of states in countering cybercrimes. This is manifested in the divergences between international and regional approaches to cybercrime and the conflicting political interests that dominate the preferences of states in the region (Thomas, 2009, pp. 19-20; Heinl, 2016, 2018). Another challenge is that region institutions have minimal influence on the state behaviour and cannot moderate the impact of the imbalance distribution of capabilities in the region (Mearsheimer, 1995, p. 7). In this regard, regional cooperation is limited because institutions cannot compel cyber powers to share their knowledge and resources regarding digital forensics or advance cyber threat analytics for instance, with less powerful states.

### *Critical Infrastructure Protection*

Protecting Critical Information Infrastructure (CII) against computer network attacks figures prominently in the cybersecurity of New Zealand, Singapore, and Brunei. Since infrastructures are vital in the functioning of society and economy, shielding these infrastructures from cyber incidents is integral to the national security of states. States with sophisticated CII have therefore more incentives to develop capabilities for computer network operations given the necessity of defence against the full spectrum of cyber threats affecting highly networked states (Slayton, 2017, p. 94). The development of CII is influenced by the uneven distribution of power since states with more material resources build more advanced CII to ensure efficient and secure government services as well as sustainable economic development. In this context, it is vital for highly networked small states to build robust infrastructures to reinforce their cyber defences and compensate for their lack of military capabilities relative to other states in the region.

Singapore has the most advanced CII among the three states. The Singapore Government's efforts to develop resilient infrastructures are a critical component of its strategy to respond to cyber conflict. The state is focused on four initiatives. The first is the defence of essential services through the implementation of a CII Protection Programme and promotion of Security-by-Design practices (Cyber Security Agency [CSA], 2016, p. 13). The CII Protection Programme aims to enable information exchange among CII operators and promote a culture of "cyber risks literacy" across all levels of each organization while Security-by-Design practices strengthens the defence of basic services by building security features into the software and control systems during the early stages of software and system development (McGraw, 2013). The second initiative is bolstering Singapore's response to cyber threats through four measures: enhancing situational awareness; implementing cybersecurity exercises; expanding the National Cyber Incident Response Teams; and reinforcing Disaster Recovery Plans and Business Continuity Plans of essential services in preparation for cyber incidents (CSA, 2016, 17).

The third is modifying governance and legislative frameworks to address cyber threats. Singapore's *Computer Misuse and Cybersecurity Act* is an appropriate framework for investigating cybercrimes but this law does not support a pro-active approach to cybersecurity. The Singapore Government has therefore initiated the creation of a new law that "will establish a comprehensive framework for the prevention and management of cyber incidents, and complement the existing laws (CSA, 2016, p. 19). The fourth initiative is to strengthen government networks through four measures: increase government expenditure on cybersecurity, reduce the attack surface of government systems, enhance cyber situational awareness in the government, and sharpen cyber incident management. These systematic initiatives to protect infrastructures are consistent with Singapore's objective of securing its networked-enabled economy and society (CSA, 2016, p. 4). The state's strong reputation for strong cyber defence is instrumental in dissuading more powerful adversaries in the region from utilising cyber capabilities to compromise the national security of Singapore.

New Zealand identifies the protection of CII as a main priority but its initiatives are not as elaborate as Singapore's because it has less capacity to and experience with managing complex cyber threats. The Government efforts are concentrated on two initiatives: improving capabilities for cyber defence and supporting private organisations. New Zealand's approach in enhancing national defensive capabilities is encapsulated in Cortex, a government project designed to counter cyber threats. While Cortex upgrades the defensive capabilities of GCSB, the operational benefits of the programme extends to a limited number of government agencies and consenting private sector organisations of national significance from foreign-sourced, technically advanced, and persistent malicious software (GCSB, 2014a, p. 1-2). Cortex directly contributes to the protection of CII by allowing specified organisations access to early detection measures; targeted advice on the prevention and mitigation of cyber threats; identification of vulnerabilities in computer systems and networks; mitigation of advanced malicious software (GCSB, 2015, p. 4).

The second initiative focuses on supporting the capabilities of private organisations particularly Internet Service Providers (ISPs) in counter cyber incidents. Private operators of CII are instrumental to the state's cyber strategy because these are priority targets of adversaries and are connected to secure government computer networks. Indeed, computer network attacks conducted by China, North Korea, and Russia against states in the region have targeted private organisations managing CII, which in turn affected other essential government services (Blank, 2008; Baker et al. 2010; Jun et al. 2015). Considering these circumstances, New Zealand's intention to strengthen its infrastructure is consistent with its objective to protect its expanding digital resources and moderate the impact of the imbalanced distribution of cyber capabilities between states in the region by developing robust cyber defences.

Brunei recognises the contribution of CII in building a sustainable economy and dynamic society but its efforts towards CII protection are still incipient, focused on upgrading and expanding its *National Digital Strategy 2016-*

*2020*. In this context, Brunei's strategy for strengthening CII concentrates on three components: developing cloud services; establishing the National Data Centre; and upgrading national broadband services (Brunei Ministry of Communications, 2016, pp. 51-52).

These priorities differ from the actions implemented by Singapore and New Zealand because these do not directly relate to CII protection. However, Brunei's efforts to improve its digital environment and government systems reflect the need to catch up with the technological developments in the region. Although the state remains mindful about the social and political ramifications of increased engagement with network technology, it has no choice but to manage the impact of the power imbalance by enhancing its network readiness and look into the development of cyber capabilities. The imbalance in capabilities and resources has compelled Brunei to adapt to the existing strategic environment by advancing its CII in line with the practices of other states in the region. Brunei's detachment from any territorial disputes and political rivalries in the region does not make it immune from computer network attacks giving the state more incentives for developing cyber capabilities as well as a strategy to guide cyber operations.

### *Diplomacy*

The transnational nature of cyber threats makes diplomacy an essential component of a formidable cybersecurity strategy. Diplomacy through international cooperation contributes to cyber strategies by promoting cyber norms, enhancing cyber capabilities, and building confidence among states (Burton, 2013; Hughes and Colarik, 2016). International cooperation is more crucial for the national security of small states given their limited material resources and military capabilities however, the diplomatic efforts of New Zealand, Singapore and Brunei reveal the limitations of cooperation in moderating the impact of the uneven distribution of cyber capabilities in the region.

The diplomatic component of New Zealand's cybersecurity strategy is the most comprehensive among the three states. The New Zealand Government advances the following initiatives in line with its national interests: (1) promote norms and "rules for the road"; (2) build networks for operational cooperation; (3) support regional capability and confidence-building measures (CBMs); and (4) maximise economic opportunities (NCPO, 2015a, p. 11). The first initiative is implemented to increase New Zealand's political influence and bargaining power in the international system by advocating for norms and rules. Through its engagement with Internet Governance Forum of the United Nations, the state has contributed to debates regarding the preservation of a free, open and secure cyberspace; application of international law in cyberspace; and governance of the Internet (Heather Ward, personal communication, June 15, 2016). New Zealand contends that norms and rules for cyberspace can minimise uncertainty and mistrust because these will shape the expectations about cyber interactions.

The second initiative focuses on developing international operational cooperation networks to improve the cybersecurity capabilities of government agencies. New Zealand's participation in joint cyber incident response management and crisis response exercises with international partners such as the Asia Pacific Computer Response Team (APCERT) enables operational agencies to supplement existing expertise on the protection of networks and investigation of cyber threats (NCPO, 2015a, pp. 10-11). The third initiative involves supporting regional capability and CBMs. A key aspect of this initiative is New Zealand's contribution to improving the cyber capabilities of states in the Pacific Islands. In line with this, New Zealand supports states in the Pacific Islands by assisting governments to address cyber crimes and boosting Internet connectivity necessary for economic development (New Zealand Ministry of Foreign Affairs and Trade [MFAT], 2015, pp. 10 and 13). New Zealand's motivation of assisting in capacity building is mainly humanitarian in nature particularly improving the economic development of the Pacific Islands states through better Internet connectivity as well as cybersecurity.

Another aspect is New Zealand's push for cyber CBMs in the region through the ASEAN regional Forum (ARF) and its key partners like Australia. The current geopolitical environment in the region necessitates CBMs to diffuse tension and uncertainty over the unequal development of cyber capabilities, incidence of cyber conflict, and the prevalence of cybercrime (Feakin et al., 2015; Limnéll, 2016). In this sense, New Zealand has taken the lead in promoting dialogue regarding cybersecurity issues in the Asia-Pacific (Parameswaran, 2016). Building capability and confidence supports international cooperation since it is a sincere effort to promote transparency between states in the area of cybersecurity.

The last initiative is maximising economic opportunities generated from technology-enabled innovation. The limited income produced from harvesting natural resources has influenced New Zealand to focus on developing range of services that depend on ICT. The services sector, which includes professional services, finance and insurance, and media and telecommunications, contributes the highest share in New Zealand's gross domestic product (New Zealand Ministry of Business, Innovation and Employment [MBIE], 2014, p. 32). Given the significance of services, strong international networks are necessary to establish the state's international credibility for cybersecurity and ensure trading partners that all online business and intergovernmental transactions with New Zealand's are safe (NCPO, 2015a, pp. 10-11).

The diplomatic initiatives in Singapore's cyber strategy are parallel to New Zealand initiatives since it centres on three initiatives: international networks, regional capacity building, and promotion of norms and laws. More specifically, the efforts centre on: (1) forging international networks to counter cyber threats; (2) advancing cyber capabilities through ASEAN; and (3) facilitating dialogue regarding norms and legislation for cyberspace. The first involves cooperating with ASEAN partners through increased information sharing and skills training to develop a collective, more coordinated approach in countering cybercrime in the region. In addition to regional cooperation, the Singapore Government also draws on the resources of international institutions such as the INTERPOL and APCERT. These institutions are instrumental in Singapore's drive to enhance its capabilities in incident reporting and response linkages (CSA, 2016, pp. 45-46).

The second initiative aims to build the capacity of ASEAN Member States in the area of cybersecurity. Similar to New Zealand's obligations with the Pacific Island Forum, Singapore considers ASEAN as a key player in addressing cyber threats in the region where powerful states are actively engaged in cyber conflict. The state is therefore committed to raising cybersecurity awareness through workshops and conferences as well as conducting training and exercises to increase the technical and operational capacity of its neighbours through the establishment an ASEAN Cyber Capacity Programme to complement existing initiatives (CSA, 2016, p. 45).

Facilitating exchanges regarding cyber norms and legislation is the third initiative. Singapore recognises that the transnational nature of cyber threats can only be mitigated through interstate cooperation. The regional platforms implemented for this initiative are the ASEAN Ministerial Conference on Cybersecurity and the International Cyber Leaders' Symposium both launched to stimulate "global and regional dialogues on cyber norms building and codes of conduct, cyber policy and legislation, cyber deterrence and cybercrime cooperation" (CSA, 2016, p. 47). Bearing in mind the barriers in developing cyber norms and legislation, these initiatives are essential for both capacity building and CBMs between states. Building the capacity for cyber operations is crucial for mitigating the uncertainty regarding the uneven distribution of cyber capabilities in the region because it enables less powerful states to defend their computer networks without necessarily depending on great powers. CBMs allow states to increase cooperation by working towards a degree of transparency regarding their capabilities and intentions in cyberspace.

Brunei's diplomatic initiatives towards cybersecurity are limited compared to New Zealand and Singapore. Collaboration with institutions and strategic partners is not explicitly discussed in any of the state's government strategies relating to ICTs and there is no clearly identified government programme for international cooperation in the area of cybersecurity. Whereas New Zealand and Singapore have expressed well-defined preferences regarding cyber norms and rules, Brunei has not actively articulated its position in this area (Haji Bakar, 2014). An explanation for this behaviour is the state's preference for a controlled digital environment to mitigate political dissent and restrict any contradictions to its national ideology.

A strong indicator that reinforces this explanation is Sultan Hassanal Bolkiah's apprehensive view of globalisation and the Internet: "We must be wise and cautious in reaping its benefits. Otherwise, if we are careless and abuse (this technology), the adverse effects will not just be on the individual but on the nation as a whole" (BPMO, 2014). Another indicator is the use of "an informant system" to monitor suspected dissidents that disseminate subversive content or ideas that challenge the national ideology through the Internet (Freedom House, 2014; Müller, 2015, pp. 319-320). While Brunei supports a state-driven framework for Internet governance, aggressively advocating for this position may have negative implications on its domestic affairs considering the Sultanate's efforts to take advantage of networked technologies to remain in power. Despite these gaps, Brunei's increasing dependence on ICTs for government and private transactions has forced its leadership to upgrade its capabilities and thereby necessitating engagement with international institutions (Brunei Ministry of Communications, 2016).

The state benefits from its membership with the International Multilateral Partnership Against Cyber Threats (IMPACT) initiative, a global public-private platform established under the International Telecommunications Union (ITU). IMPACT is central for Brunei's cybersecurity efforts because it provides response assistance, research support, and training programmes "to address internet-related crimes that are targeting those who are young and vulnerable within society" (Haji Bakar, 2014). Although Brunei supports regional efforts to address cyber threats through its participation in ASEAN-Japan Information Security Meetings, there is no evidence to suggest that it has introduced any specific cybersecurity initiative in the region such as New Zealand's advocacy for cyber norms and Singapore's coordination of the ASEAN Ministerial Conference on Cybersecurity.

## Cyber capabilities and conventional military forces

The promise of the information revolution has influenced states to develop and integrate capabilities for computer network operations to upgrade their military forces and gain the strategic advantage over adversaries (Nye and Owen, 1996). The modernization of military forces involves upgrading antiquated weapon platforms and subsystems to new military hardware that depend on networked systems to function properly. The shift to new weapons platforms and subsystems is more prevalent in the Asia-Pacific Region where the majority of states are currently upgrading their military forces to mitigate the impact of the unequal distribution of military capabilities in the region, compounded by territorial disputes and historical animosities between rival states.

The discrepancy in the distribution of power has shaped the development of cyber capabilities in the region with great powers such as China and the U.S. leveraging on the strategic advantages of emerging military technology by racing to develop capabilities, organizations, and doctrines focused on military cyber operations (Manson, 2011; Domingo, 2016). In response to these actions, middle powers such as Australia and South Korea have upgraded their existing cyber capabilities with the objective of protecting their computer networks from intrusions as well as complementing their capable military forces (Tan, 2011;

Raska, 2011). Small states meanwhile have invested in military cyber capabilities to defend their military networks and align capabilities with foreign policy objectives. Following these developments, this section explores the link between computer network operations and conventional military capabilities in New Zealand, Singapore, and Brunei. Whereas the previous section that surveyed the role of the military within the broader cyber strategies of small states, this section continues the analysis by specifically focusing on the contribution cyber capabilities in the military affairs.

In relating these capabilities, the section builds on existing literature that links the development of cyber capabilities to a state's foreign policy alignment and capacity to make use of new military technology. Since cyber capabilities are typically developed as part of a broader set of information technology-driven military capabilities, it is useful to situate cyber operations as part of the Revolution in Military Affairs (RMA) (Goldman, 2004; Halpin, et al., 2006; Raska, 2011a). The RMA thesis contends that "advances in precision munitions, real-time data dissemination, and other modern technologies can help transform the nature of future war and with it the size and structure" of military forces (O'Hanlon, 2000, p. 7).

Important studies by Dibb (1997), Goldman and Mahnken (2004), and Tan (2011, 2014) suggest that states closely allied with the U.S. are oriented towards the RMA. A strong alliance with the U.S. has convinced less powerful states in the region to invest in networked systems that integrate a range of military functions including intelligence, surveillance, and reconnaissance (ISR); command, control, communications and computer processing (C4); logistics support; and complex combat systems. In this sense, cyber operations are essential for states that have assimilated the RMA since computer networks and information systems are necessary components of military operations. Based on this argument, the link between cyber and conventional military capabilities is inconsistent in the case of New Zealand, Singapore, and Brunei as these states have different foreign policy alignments as well as different strategic preferences.

*Relating foreign policy alignment with the RMA*

The literature on military-technological innovation has established that a state's foreign policy alignment is connected to its orientation towards the RMA (Dibb, 1997). The experiences of several states in the region - Australia, Japan, South

Korea- confirm this observation since these states are part of a defence pact with the U.S. and all have modern military platforms and subsystems that are interoperable and suitable with capabilities of U.S. military forces (Goldman and Mahnken, 2004; Tan, 2014). New Zealand, Singapore and Brunei are interesting cases since their experiences are inconsistent with observations in the literature: none of these states have a defence pact with the U.S. but some are oriented towards the RMA.

New Zealand has maintained an independent foreign policy since it disassociated itself from the Australia, New Zealand, United States Security Treaty (ANZUS) in 1984 due to its nuclear-free policy that the U.S. attempted to violate. Both states have rebuilt a deeper bilateral defence relationship over the last decade with the signing of the Wellington Declaration in 2010, which focuses on security cooperation in the South Pacific, and the Washington Declaration in 2012 that emphasizes security cooperation towards the Asia-Pacific Region (Ayson and Capie, 2012). While informal allies do not benefit from any security guarantees, this status has provided New Zealand more flexibility to cooperate with other great powers such as China with the objective of alleviating the impact of the uneven power distribution in the region.

New Zealand's independent foreign policy alignment has affected its orientation towards the RMA. The NZDF acknowledges the importance of ICTs in military operations but is sceptical about the potential of the RMA: "Despite revolutionary advances in information processing and data management, knowledge, information and intelligence about an enemy or situation will remain finite and subject to probabilities" (New Zealand Defence Force [NZDF], 2012, 22). In addition, the benign strategic environment affecting New Zealand has shaped the modernisation trajectory of the NZDF towards military operations other than war more than major combat operations (Ayson, 2016). Given these circumstances, the NZDF has continued to upgrade its capabilities without necessarily adopting the extensive changes envisioned in an RMA-oriented military force.

Singapore's experience is different from New Zealand since it was never part of a defence pact with the U.S. Both states however have pursued autonomous foreign policies while preserving strategic partnerships with the U.S. through several strategic agreements. Singapore has been more systematic than

New Zealand because it has entered into a several agreements with the U.S.: Memorandum of Understanding on the use of military facilities in 1990; a Strategic Framework Agreement on principles of cooperation in 2005; and an Enhanced Defence Cooperation Agreement focusing on military, policy, strategic and technology, and nonconventional security challenges in 2015 (Singapore Ministry of Defence, 2015). Even though both states are unofficial allies, New Zealand has signified closer alignment with the U.S. while Singapore has remained ambiguous, hedging between China and the U.S. with the objective of mitigating the impact of the military capability imbalance in the region (Lim and Cooper, 2015, pp. 721-723).

The hedging strategy of Singapore has influenced its orientation towards the RMA. Singapore's flexible foreign policy alignment has exposed the state to extensive interactions with the military forces and defence industries of advanced industrial countries, enabling the small states to make substantial advances towards participation in the RMA since the 1990s. In terms of technology, the SAF has deployed increasingly sophisticated defence systems, particularly in the RMA-related areas of precision weapons, intelligence, surveillance, and reconnaissance; command, control, communications, and computer processing, and logistics support (Huxley, 2004, p. 196). In this regard, Singapore's preference for non-alignment contributes to its strong orientation towards the RMA since cutting edge military technology is necessary for the state to maintain the strategic edge or a "one generation" lead over other military forces in the region (Bernard Loo, personal communication, July 27, 2016).

Brunei's autonomous foreign policy alignment is similar to New Zealand and Singapore. The state is not part of a defence pact with any great power but has maintained durable defence relations with the U.S. This officially started in 1994 through a Memorandum of Understanding on Military Exchanges but continues to enhance its limited military capabilities through constant exercises with the U.S. (Chwee-Kuik and Welsh, 2005, pp. 63-64). A crucial difference with New Zealand and Singapore however is Brunei's direct involvement in the territorial dispute in the South China Sea since it is one of the five claimant states (Brunei Ministry of Defence, 2011). Despite these longstanding territorial disputes, Brunei has not signified any intention of asserting its claim nor has it reoriented its foreign policy to pursue an official alliance with the U.S. or China.

In this regard, Brunei's hedging strategy is similar to Singapore's however, the major difference is the absence of a highly capable military force used for deterrence and power projection in the region.

Despite having a similar alignment to Singapore, Brunei has not responded favourably to the RMA. Although the RBAF trains constantly with the most advanced military forces and Brunei has invested around 3% of its GDP on defence in the last ten years (World Bank, 2017), the state has yet to implement extensive upgrades in the RBAF (Banaloi, 2009). More relevantly, the state is not inclined to adhere to the changes advocated by the RMA since its defensive strategy focuses on international institutions, economic cooperation, and bilateral relations with powerful states thereby downplaying the significance of building a technologically superior military force (Chwee-Kuik and Welsh, 2005, pp. 62-63). Nevertheless, the state recognises the strategic advantages of networked military technology in coping with the uncertainty driven by the relative distribution of capabilities in the region. The importance of ICTs is captured in Brunei's *Defence Policy Framework,* which identifies capabilities for ISR and knowledge integration as essential elements in the RBAF's strategy to address the geopolitical tension and technological vulnerabilities that affect the state (Brunei Ministry of Defence, 2011, p. 3). There is no clear evidence however, about the extent to which these networked technologies have been integrated within the RBAF and the strategy to employ these technologies as strategic instruments to manage the power imbalance between states in the region.

### *Cyber capabilities and military operations*

The inconsistent link between foreign policy alignment and the response to the RMA in the three small states implies that binding security agreements with great powers are not necessarily compelling factors that influence less powerful states to develop cyber capabilities. Building on these observations, it is now possible to explore the contribution of cyber capabilities in conventional military operations. This section draws on Goldman's (2004) work that clarifies the impact of ICTs on military performance. She contends that ICTs facilitate military performance through four "discursive functions": efficiency, intelligence, coordination, and transformation (Goldman, 2004, pp. 207-208). These functions are helpful analytical categories to explicate the contribution of cyber capabilities in conventional military operations essential for coping with the relative distribution of power in the region. Since the military transformation of the three states has already been examined through the RMA engagement of three states, this section will only explore the first three categories.

The *efficiency* facilitated by ICTs is enhanced in military operations through speed of delivery or the near instantaneous nature of cyberspace (Sheldon, 2011). This function is essential to military forces of New Zealand, Singapore, and Brunei since these states have invested in modern military platforms that run on networks such as combat management systems for warships and maritime surveillance systems for patrol aircrafts. However, the efficiency derived from ICTs is uneven between the three states considering the different types of military operations undertaken by each state.

New Zealand has configured its military for operations other than war in view of its non-threatening strategic environment. Cyber capabilities are therefore employed to protect computer networks and communications channels during humanitarian assistance, disaster relief, and peace operations (Richard Elwin, personal communication, June 17, 2016). Nonetheless, the significance of computer network operations will increase quickly as the NZDF's capabilities have been constantly upgraded in the areas of ISR (surveillance aircraft sensors and communications), strategic communications (enhanced satellite communications), and command and control (inter-service information sharing) (New Zealand Ministry of Defence, 2014, pp. 36-27)

Singapore's use of ICTs is much more elaborate than New Zealand since the state has developed the full spectrum of cutting-edge military capabilities in preparation for potential conflict scenarios in the region. The efficiency derived from ICTs is manifested in deployment of airborne early warning and control systems as well as ISR platforms that strengthen the SAF's situational awareness and intelligence collection capabilities. More significantly, Singapore's acceptance of the Integrated Knowledge-based Command and Control (IKC2) doctrine in 2005 further solidified its reliance on computer networks, enabling the SAF to share real-time information across all units as well as enable comprehensive situational awareness to improve decision-making (Singapore Ministry of Defence, 2005). The implication of these advancements is paradoxical: it enables to the SAF to deploy cutting edge military platforms and subsystems but it also exposes its networks and computer systems to cyber intrusions by more capable states. The vulnerabilities associated with strong dependence on network technologies have motivated Singapore's aggressive approach to managing cyber insecurity in the region, particularly through the establishment of the Defence Cyber Organisation.

Similar to New Zealand, Brunei's military forces are not organised to engage in major military combat operations since the state is not threatened by any foreign power and has no reason to build a technologically superior military. In this context, the RBAF has the least opportunity to benefit from the efficiency facilitated by ICTs because its military platforms and subsystems are still under development and there is no evidence to suggest that its modernisation trajectory is aligned with Singapore or any other RMA oriented state. While it is still uncertain if the RBAF has developed cyber capabilities however the main function of these capabilities would be limited to the protection of military networks more computer network attacks and exploitation (Brunei Ministry of Defence, 2011).

Another function is that ICTs facilitate the collection of *intelligence*. Espionage through the use of computer networks is favourable for states given the low risks and high potential of obtaining adversaries' secrets. There is no physical damage or harm because spies operate behind computers in secure government buildings, infiltrating target networks in different states (Clemente, 2014, p. 256). In the military context, computer network exploitation is not limited to gaining insights about the adversaries' capabilities and intentions but is crucial for developing a well-calibrated military cyber strategy in the most active region for cyber conflict (Walsh and Miller, 2016, pp. 356-357). Public information about the use of technology for military intelligence are limited in the case of New Zealand, Singapore and Brunei but available evidence suggests that their military forces are using ICTs for intelligence purposes. Two implications can be drawn from the limited information disclosed about military intelligence operations in cyberspace. First, the prevalence of computer network exploitation by great powers has influenced less powerful states to emphasise the defensive aspects of their military cyber capabilities such as strengthening detection systems and protecting of information infrastructure. Second, some small states are reluctant to disclose more information about their military cyber capabilities because they have not fully explored the impact of these technologies on their military forces.

Monitoring and assessing New Zealand's strategic environment is a core mandate of the military. Therefore, the Ministry of Defence has ensured that the NZDF "will maintain a range of land and naval combat, strategic projection and logistics, intelligence and reconnaissance capabilities" (New Zealand Ministry of Defence, 2016, p. 12). Intelligence in this view is collected through different sources and is considered part of a fundamental set of military capabilities (i.e. ISR sand C4), often developed for enhancing the operational decision-making capacity of military leaders. However, the NZDF's computer network operations are not explicitly discussed in any government document or by any official in the New Zealand Government.

The closest indication of NZDF's cyber capabilities is the organisation's signals intelligence (SIGINT) capabilities, which have been reinforced through its limited cooperation with other intelligence agencies of the state, particularly the GCSB. The GCSB has "provided assistance to NZDF with SIGINT testing and training through a series of ongoing exercises. By providing access to toolsets, facilities and technical knowledge, GCSB enabled NZDF personnel to maintain and improve their skills and capability" (GCSB, 2015, p. 19). In line with the NZDF's defensive orientation, it is reasonable to contend that these cyber capabilities have been developed for protecting computer networks and networked weapon systems for conventional military operations (Richard Elwin, personal communication, June 17, 2016).

The SAF's extensive investment in networked military technology extends to its intelligence collection capabilities. Intelligence collection in relation to SAF is traditionally focused on intercepting communications signals of neighbouring states. The SAF's considerable SIGINT capabilities were developed with the assistance of Israel as well as the state's capable indigenous defence industry (Ball as cited in Huxley, 2000, p. 90). Singapore initially requested military assistance from India and Egypt but was rejected because of political reasons: both states wanted to avoid any conflict with Malaysia and Indonesia. Israel was a strategic choice because aside from having the technical expertise to develop SIGINT capabilities, the state's strategy for survival in a hostile region was impressive (Tan, 1999, p. 454). In terms of cyber capabilities, the most relevant insights regarding the SAF computer network operations has been Singapore's capability to collect signals intelligence on its neighbours Malaysia and Indonesia (Ball as cited in Huxley, 2000, p. 90) as well as its recent contribution to the FVEY intelligence network which was discussed in the previous section.

Since the Ministry of Defence has confirmed the formation of a Cyber Defence Organisation, Singapore's version of a "cyber command", it is sensible to argue that the SAF is capable of computer network exploitation (Ng, 2017). Even though both states exploit computer networks for intelligence collection, Singapore's approach to intelligence collection is more aggressive and pre-emptive than New Zealand's because of the differences in their military practices and national traditions, encapsulated in their respective strategic cultures (Booth and Trood, 1999, pp. 13-14). The strategic culture of small states is crucial since it filters their responses to the relative distribution of power in the region. The role of strategic culture as a necessary secondary condition for developing cyber capabilities is discussed in the next chapter.

Brunei's use of ICTs for military intelligence focuses on providing early warning against potential threats and ensuring transparency in the area of operations. Much like NZDF and the SAF, the RBAF's intelligence capabilities are integrated within a fundamental set of military capabilities and are designed to support conventional military operations such as maritime surveillance and defence of Exclusive Economic Zones (Ball, 2004). The RBAF's employment ICTs for intelligence collection has therefore centred on SIGINT and electronic warfare capabilities with the objective of mitigating uncertainties caused the relative distribution of power in the region (Brunei Ministry of Defence, 2004). Although the Brunei Ministry of Defence has acknowledged the necessity for robust network defences, there is no evidence to confirm the RBAF's capabilities for computer network operations (Feakin, et al., 2016, p. 28).

A third function is that ICTs facilitate *coordination* within and between military forces. ICTs are central to modern military forces since computers and networks allow the rapid coordination of multiple tasks across different geographical locations (Goldman, 2004, p. 206). The development of joint forces and participation in military exercises are straightforward indicators of interservice coordination and more relevantly the need for cyber capabilities. In spite of having limited resources, the NZDF, SAF, and RBAF all have components of joint forces to strengthen the integration between military services. While assessing the level of "jointness" of each military force is beyond the scope of this study, it is clear that joint operations "are facilitated when information passes easily between different services, both within and across national militaries" (Goldman, 2004, p. 209).

Indeed, computers and networks have become indispensable for the completion of the most basic tasks in military operations (e.g. C4 and ISR) therefore it is not possible to employ joint forces without leveraging cyberspace (Williams, 2014, 12; Bezooijen and Kramer, 2015, 446). Considering this significance, both New Zealand and Singapore have developed capabilities for computer network operations to protect military computer networks and weapon systems (Richard Elwin, personal communication, June 17, 2016; Wong Yu Han, personal communication, July 28, 2016). These capabilities are reflected in New Zealand's *Defence White Paper 2016* as well as the Singapore Government's statement regarding the establishment of a Cyber Defence Organisation within the SAF. In contrast, Brunei's military cyber capabilities are still underdeveloped and there is no public information confirming the implementation of the RBAF's stated plans for strengthening computer network defence (Brunei Ministry of Defence, 2011)

A second indicator of cooperation facilitated by ICTs is engagement in military exercises. From a strategic perspective, small states typically participate in military exercises to benchmark with the military capabilities of great powers. These exercises are undertaken as part of a defence agreement between great powers and strategic partners like New Zealand, Singapore and Brunei to deter potential adversaries and upgrade military capabilities (Boon, 2015; Parameswaran, 2017). Cooperation is facilitated by technology during joint military exercises given that the central objective of these exercises is to achieve interoperability or the "the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together" (U.S. Department of Defense, 1999, p. 229).

Reaching a level of interoperability with the U.S. necessitates a significant amount of investment in technologically sophisticated military platforms that operate using computer networks and networked-enabled weapon systems. These requirements generate the need for cyber capabilities since military computer networks and weapon systems are frequent targets of network exploitation and attack by adversaries (Boland et al., 2015). In line with this predicament, New Zealand and Singapore have invested in cyber capabilities to strengthen the computer network defences and ensure that they are interoperable with the U.S. in terms of cyber operations (NZDF, 2016; CSA, 2016). On the other hand, Brunei's case is different because like Singapore, it consistently participates in annual bilateral military exercises with the U.S. (i.e. Cooperation Afloat Readiness and Training) but there is no clear evidence of cybersecurity cooperation between Brunei and the U.S. (U.S. Department of State, 2017).

Information and communication technologies strengthen conventional military operations by facilitating the rapid diffusion of information, providing an alternative method of collecting intelligence, and enabling the coordination across different aspects of military operations. Cyber capabilities are necessary to preserve the integrity of these functions particularly for small states that need to thrive in a region shaped by the imbalanced distribution of power. There are two implications that can be drawn from points raised in this section. The first is that the discrepancy between the capabilities of military forces across the region compels small states to emulate the military cyber capabilities of the most powerful states to increase their chances of survival (Goldman and Andres, 1999). The second is that since small states have limited material resources, they can only invest in limited military cyber capabilities thereby forcing them to enhance their cooperation with cyber powers in the region.

## Cyber power and small states

Cyber capabilities as an enhancement of conventional military forces are valuable components of the strategy of small states but the full potential of ICTs can be achieved from the use of cyberspace to affect foreign policy and not just military outcomes. These sets of actions can be considered as part of a state's cyber power or "the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain" (Nye, 2011, p. 123). Existing studies contend that the use of cyber power is attractive for small states given the intrinsic limitations in material resources as well as ability to advance their foreign policy interests in the international system (Nye, 2011; Burton, 2013;

Areng, 2014; Valeriano and Maness, 2015). This observation is more profound for small states in the Asia-Pacific Region where the relative distribution of power favours powerful states that have extensive resources, enabling them to exercise overwhelming cyber power (Nye, 2010, p. 3).

Following the emerging literature on cybersecurity and small states, this section explores the contribution of cyber power to the foreign policy of small states. Whereas the focus has been the strategic or military aspect of cyber power, a balanced analysis of the cyber strategy of small states necessitates a wider conception that considers cyber power as part of "a variety of powers that circulate in cyberspace and which shape the experiences of those who act in and through cyberspace" (Betz and Stevens, 2011, p. 44). With this in mind, this section draws on the work of Betz and Stevens (2011) who applied Barnett and Duvall's (2005) taxonomy of power to come up with a systematic evaluation of cyber power. This taxonomy is a useful conceptual framework because it presents two analytical dimensions the capture the essence of power: "the kinds of social relations through which power works; and the specificity of social relations through which effects on actors' capacities are produced" (Barnett and Duvall, 2005, p. 44). This study builds on these works by exploring four distinctive forms of cyber power (i.e. compulsory, institutional, structural, and productive) and evaluating how these conceptions of power relate to the strategies employed by selected small states in managing the impact of the uneven distribution of power in the region.

*Compulsory*

The first form of cyber power involves the use of direct hostile action by one state in an attempt to change the behaviour and conditions of existence of another through computer network operations. This form is compulsory in the sense that victims are compelled to do the will of aggressors (Betz and Stevens, 2011, p. 45). Dahl's (1959, pp. 202-203) conception of compulsory power is useful in this context: "*A* has power over *B* to the extent that he can get *B* to do something the *B* would otherwise not do." Several examples of this form of cyber power are manifested in different cyber conflicts between states in the region including China and Japan, North Korea and South Korea, and India and Pakistan (Valeriano and Maness, 2015, pp. 88-89).

The contribution of compulsory cyber power to foreign policy strategy can be determined by matching ideas prescribed by the concept with a state's *capabilities* (i.e. military capabilities) and *intentions* (i.e. foreign policy behaviour). New Zealand's capabilities and intentions are not consistent with the ideas presented by compulsory cyber power. In terms of capabilities, New Zealand maintains an efficient defence force but it has been consistently constrained by the limited resources allotted by the government predominantly due to New Zealand's strategic culture (McCraw, 2011). The NZDF is currently enhancing its cyber capabilities but these are specifically developed to support a range of engagements including military operations other than war in addition to combat operations (NZDF, 2016; Richard Elwin, personal communication, June 17, 2016).

In terms of intention, New Zealand has developed an independent foreign policy alignment, disengaging with the ANZUS Treaty but developing a stronger, renewed relationship with the U.S. during the past seven years. More relevantly, despite of its non-alignment, New Zealand has managed a robust relationship with influential states through its participation, via the GCSB, in the FVEY intelligence network (Patman and Southgate, 2016, p. 874). While it is possible that the GCSB is capable of the full range of computer network operations, several sources indicate that the primary role of the agency has been to collect signals intelligence and not to execute offensive cyber operations against adversaries (Kitteridge, 2013; Heather Ward, personal communication, June 15, 2016; Anthony Smith, personal communication, June 17, 2016). In summary, compulsory cyber power has low potential for New Zealand's foreign policy for two reasons. First, conducting hostile actions in cyberspace will not be consequential for the state since it does not have sufficient military capabilities to support its cyber operations in the event of escalation to conventional military conflict. Second, New Zealand has no intention of conducting computer network attacks therefore decreasing the potential for hostile actions against adversaries in the region.

Singapore's military capabilities are more advanced than most states in the region but the state's intentions are not compatible with the ideas presented by compulsory cyber power. In contrast with New Zealand, Singapore maintains a highly capable and technologically superior military force, supported by extensive resources allocated by the government. As discussed earlier, the SAF's orientation towards the RMA necessitates the development of cyber capabilities to protect military computer networks and weapon systems. More significantly, the on-going development of the Cyber Defence Organisation within the SAF is a clear manifestation of Singapore commitment to building formidable cyber capabilities.

In terms of intention, Singapore pursues an independent foreign policy alignment similar to New Zealand but does not maintain any official defence or intelligence sharing commitments with any great power. This is consistent with Singapore's hedging strategy, which makes the state more flexible in pursuing its national interests through participation in different types of bilateral and multilateral arrangements with China, the U.S. as well as their respective allies. Based on these circumstances, compulsory cyber power has moderate potential for Singapore's foreign policy strategy because of two reasons. Firstly, despite Singapore's strong interest in enhancing its military cyber capabilities, these exist only to support the SAF's operations through network defence and intelligence collection (CSA; 2016; Ng, 2017). Secondly, using cyber operations to alter a state's behaviour weakens Singapore's foreign policy strategy since the purpose of hedging it to increase a small state's chances of survival and not create opportunities for cyber conflict against adversaries.

Brunei's military force is one of the smallest in the region and the state's foreign policy behaviour contradicts with the ideas presented by compulsory cyber power. In contrast to the NZDF and the SAF, the RBAF's capabilities are limited not necessarily because of a lack of resources but rather non-threatening strategic environment, which is a disincentive for the state to develop a more formidable military force. Brunei recognises the significance of cyber threats however, its capabilities are still underdeveloped and are far from what Singapore and even New Zealand are capable of (Feakin, et al., 2016).

Similar to Singapore, Brunei pursues an independent foreign policy alignment that it implements through a hedging strategy. The state maintains enduring strategic partnerships with China and the U.S. as well as other influential states such as the U.K. (Cheng-Chwee and Welsh, 2005, 64; Brunei Ministry of Foreign Affairs and Trade, 2006). A key distinction between the foreign policy entanglements of Brunei and the two other small states is its direct involvement in territorial disputes in the South China Sea. Brunei along with five other states including China, have overlapping claims to certain areas of the South China Sea that has evolved into a contentious dilemma, affecting the geopolitical landscape in the region (e.g. Rahman and Tsamenyi, 2010; Fravel, 2011; Scott, 2012). Based on these circumstances, compulsory cyber power has low potential for Brunei's foreign policy strategy because of two reasons. First, hostile actions in cyberspace will be detrimental for Brunei since its military capabilities are insufficient to support its cyber operations in the event of an escalation to conventional military conflict. Second, Brunei's foreign policy behaviour indicates that it has no intention of using coercive means to achieve its interests.

*Institutional*

The second form of cyber power involves indirect control of the state by another and this is conducted primarily through the intervention of formal or informal institutions. The intermediary institution may be influenced by a specific state to direct and constrain the actions or inactions and conditions of existence of others without being totally controlled by any state (Betz and Stevens, 2011, p. 47). Institutional power therefore exists when *A* is able to exercise power over *B* indirectly using intermediary institutions. Prominent examples of this form of cyber power can be observed in the efforts of states to promote norms for cyberspace through the United Nations as well as the promotion of a multi-stakeholder approach to Internet governance through institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN) (e.g. Maurer, 2011; DeNardis, 2014; Nocetti, 2015).

International cooperation through the development and facilitation of cyber norms, figures prominently in the cybersecurity strategies of both New Zealand and Singapore but not in the case of Brunei.  A core aspect of New Zealand's cyber strategy is ensuring that Internet governance is consistent with its national interest of maintaining "a free, open and secure cyberspace" (NCPO, 2015a, pp. 10-11). Moreover, the state is also an active contributor to intergovernmental debates regarding the application of international law online, "including how to manage national security interests and human rights obligations in cyberspace" NCPO, 2015a, pp. 10-11). These interests are vigorously promoted through New Zealand's constant participation in international discussions facilitated by institutions such as the ICANN, Internet Governance Forum, and the Freedom Online Coalition.

Singapore also collaborates with international institutions to pursue its agenda of mitigating cybercrime and cyber capacity building initiatives in the region. The state cooperates with ASEAN to boost cyber incident reporting in the region and makes use of INTERPOL's global operational networks and capabilities to mitigate the prevalence of cybercrime in the region (CSA, 2016, pp. 44-45). In addition, Singapore leads cybersecurity capacity building initiatives within ASEAN particularly in "operational, technical, legislative, cyber policy and diplomatic areas" while advocating cyber CBMs within the more inclusive ARF (CSA, 2016, pp. 45-47).

Singapore's approach however, differs from New Zealand because it is more proactive in coordinating the development of cyber norms and standards. This difference can be attributed to the state's culture of insecurity that is manifested in its interest to build a strong strategic posture in cyberspace. This argument is discussed thoroughly in Chapter 5. For instance, Singapore has established the Singapore International Cyber Week (SICW) to promote exchanges on current and emerging cyber issues relevant to the international community while New Zealand relies more on its participation in the United Nations and Internet Governance Forum to achieve the same objectives. Nonetheless, it is clear that institutional cyber power has high potential for both states for two reasons. First, leveraging on international institutions is a proven strategy for small states to advance their foreign policy interests therefore this strategy may be useful when tackling cybersecurity issues (Burton, 2013). Second, since cyber conflict is characterised by restraint and regionalism, institutions in the region can play an instrumental role preventing escalation or just maintaining the status quo (Valeriano and Maness, 2015).

Brunei's participation in international and regional institutions is not very different from New Zealand and Singapore however there is no evidence of the state's active contribution or independent initiatives in the area of cybersecurity (ITU, 2015, p. 106). Even though Brunei benefits from the assistance of several international institutions including the ITU and contributes to cybersecurity discussions within the ASEAN., Brunei has not released any statement or document that clarifies the strategic value of institutions in protecting the state from cybersecurity threats and mitigating uncertainty in the region. Based on these circumstances, institutional cyber power has low potential for Brunei primarily because the state has yet to consider ICTs as a source of potential influence and power for small states unlike New Zealand and Singapore.

### *Structural*

The third form of cyber power concerns structures in which all states are located and which enable or limit their actions relative to their structural position with other states. The concept of structure is considered as an internal relation or "a direct constitutive relation such that the structural position *A* exists only by virtue of its relation to structural position *B*." (Barnett and Duvall, 2005, pp. 52-53). This conception of cyber power is not helpful for exploring how small states use cyberspace to achieve their interests but is useful for understanding how cyberspace helps determine structural positions (Betz and Stevens, 2011, pp. 48-49). Since small states are not capable of constituting or changing structural positions in the international system, the challenge for these states is to navigate through existing structures using ICTs. Determining how small states respond to structural cyber power is a more relevant task for this section.

An example offered by Betz and Stevens (2011, pp. 49-50) is the contribution of ICTs in building a network society or a society "where the key social structures and activities are organized around electronically processed information networks" (Castells, 2001). A network society contributes to structural cyber power because it facilitates the rapid globalization of capital (e.g. commercial online transactions) among states, which in turn preserves existing economic structures such as capital and labour. In this sense, this type of society maintains the status quo by favouring highly industrialised states that derive the most advantages from the use of networks and technology (Baller, et al., 2016). Building on this example, both New Zealand and Singapore have managed the impact of structural power by transforming their ICTs assets as cores driver for enhancing economic growth.

New Zealand has harnessed the benefits of a network society by strengthening the development of technology-oriented services, which as mentioned previously is already an important source of the state's national income. A concrete manifestation of New Zealand's efforts is the steady growth of local start-ups and multinational companies during the past decade. These firms specialise in delivering ICT services such as software development, business applications, infrastructure outsourcing, data centres as well as develop a range of ICT products for niche industries including corporate governance, geothermal, and national security among others (MBIE, 2015, 2017). Singapore has also capitalised on the advantages of a network society by building up its existing cybersecurity industry. Since the state is already home to many leading cybersecurity companies as well as emerging local start-ups, it is committed to extending this advantage by implementing four measures. The first is to attract more companies with innovative cybersecurity capabilities. The second is to support start-ups through a strong network of venture capitalists and entrepreneurs. The third is to develop local "champions" who can compete globally in area of cybersecurity. The last measure is to provide resources to enable companies to access new market segments as well as promote "Made-In-Singapore solutions" (CSA, 2016, p. 38).

Structural cyber power is pervasive and places less powerful states at a disadvantage. The initiatives pursued by New Zealand and Singapore confirm the ability of small states to adapt to and mitigate the impact of economic structures by proactively transforming their networks into an instrument of economic growth rather than a source of weakness. Brunei's experience however is not consistent with the success of New Zealand and Singapore. Despite being a highly networked state, Brunei's initiatives in harnessing the economic and strategic advantages of ICTs are still in progress, with the state pushing for digital transformation to "make government services simpler, faster and more accessible" in the next two decades (BPMO, 2015, pp. 1-5). Based on these circumstances, it is reasonable to argue that Brunei's gradual engagement towards a network society is influenced by the beliefs and practices of the state, which is encapsulated in its strategic culture.

### *Productive*

The fourth and last form of cyber power relates to the production of social capacities of states produced through discourse. Cyberspace is fundamentally an information environment therefore, it is favourable for the transmission of productive cyber power. More specifically, productive cyber power is expressed through “the constitution of subjects through discourse mediated by and enacted in cyberspace, which therefore defines the ‘fields of possibility’ that constrain and facilitate social action” (Betz and Stevens, 2011, pp. 50-51). An expression of productive cyber power is the use of soft power by states to achieve foreign policy objectives. Soft power or the “the ability to affect others through the co-optive means of framing the agenda, persuading, and eliciting positive attraction in order to obtain preferred outcomes” has been a instrumental component of foreign policy making since the end of the Cold War and has been accentuated by the rapid diffusion of information through cyberspace (Nye, 2011, pp. 20-21). While states continue to exploit the advantages of power projection through cyberspace, these advantages are not necessarily as instrumental for small states that are constrained from effectively shaping preferences of other states through soft power (cf. Nye and Keohane, 1998; Lindsay, 2013; Valeriano and Maness, 2015). Small states such as New Zealand and Singapore have been consistent in using cyberspace as a medium for soft power projection whereas Brunei’s different orientation towards ICTs has prevented it from deriving strategic advantages from cyberspace.

The strategies implemented by both New Zealand and Singapore in framing cybersecurity as a regional and global issue of concern are clear manifestations of soft power and the potential of productive cyber power. New Zealand’s foreign policy strategy of advocating for international cyber norms such as Internet freedom and multi-stakeholder Internet governance is consistent with the role of  “norm entrepreneur” or a state that “attempt to convince a critical mass of states to embrace new norms” (Finnemore and Sikkink, 1998, p. 895). These efforts directly relate to productive cyber power since potential cybersecurity norms are dispersed across different states through the discourse generated from the social interactions between technical, law enforcement, and military communities (Dunn Cavelty, 2015). Whilst disseminating norms and ideas is important for mitigating cyber conflict and uncertainty in the region, these initiatives have limited impact on state interactions considering that the interests of powerful states are likely to prevail over New Zealand’s ideal set of norms and standards for cyberspace (e.g. Stevens, 2012; Noecetti, 2015; Farell, 2015). Nevertheless, productive cyber power has high potential for New Zealand since international cooperation is a core foreign policy strategy for the state given its intrinsic limitations in material resources as well as capacity to influence other states (Burton, 2013, pp. 217-221).

Whereas New Zealand's strategy centres on promoting norms and standards for cyberspace, Singapore has been preoccupied with building a Smart Nation as a strategy to overcome the limitations as a small state. The Smart Nation initiative is a foreign policy strategy that can be a conceptualised as soft power and expressed through the medium of "virtual enlargement" or enhancing the importance of small states through non-coercive means (Chong, 2010, p. 385). Singapore's Smart National initiative is a national effort to build "a nation where people live meaningful and fulfilled lives, enabled seamlessly by technology, offering exciting opportunities for all" (Lee, 2014).

The initiative is an illustration of virtual enlargement since it showcases the advantages of a networked society while attracting other states to consider investing in ICTs for national development. More significantly, Smart Nation relates to the broader concept of productive cyber power because the initiative has generated influential discourse for innovation and cutting-edge technological advancement that has solidified Singapore's reputation as a leading financial and technology hub in the Asia Pacific region (Kevin Kwang, personal communication, July 15, 2016). Following its efforts towards virtual enlargement, productive cyber power has high potential for Singapore because it makes an important contribution to foreign policy by empowering the state to confront the geopolitical challenges without engaging in coercive actions.

Brunei's demonstration of productive cyber power has considerably low potential compared to New Zealand and Singapore. There are three points to support these assertions. First, it is not clear if Brunei intends to make use of cyber power as part of its foreign policy strategy unlike New Zealand and Singapore. Indeed, the state acknowledges the significance of investing in ICTs to develop a vibrant economy, empower citizens, and implement efficient government services; however, the initiatives designed to harness these advantages are still being developed (Brunei Ministry of Communications, 2015, pp. 38-42). Second, the discourse behind Brunei's drive towards a digital government is shaped predominantly by domestic rather than international factors (Chwee and Welsh, 2005, p. 64). This is reflected by the government's efforts in preserving the legitimacy as well as ensuring that the Sultanate of Brunei adapts to the technological change in the twenty-first century (Talib, 2002; Roberts, 2014). Third, as previously mentioned, Brunei is cautious about building a network society because the ideas and actions expressed in cyberspace may contradict or challenge the state's strategic culture that is principally shaped by the official national ideology the Malay Islamic Monarchy which is "a blend of Malay language, culture and Malay customs, the teaching of Islamic laws and values and the monarchy system which must be esteemed and practiced by all..." (BPMO as cited in Bouma, et al., 2010, p. 48).

## Conclusion

This chapter has elucidated the significance of the relative distribution of power as a necessary primary condition for small states to develop cyber capabilities. This condition was explored through three observable implications: strategy to address cyber conflict, the connection between cyber and conventional military capabilities, and the contribution of cyber power to foreign policy strategy. In responding to cyber conflict, both New Zealand and Singapore have designed cyber strategies that implement cybersecurity measures by engaging a wide range of crucial sectors including the military, intelligence services, law enforcement, private companies, and international institutions. Brunei's response however is incomplete relative to New Zealand and Singapore since it has yet to develop an explicit cyber strategy that clarifies how the state intends to systematically mitigate cyber threats. A key point that stands out in the first section of is the needs for states to develop a cyber strategy that considers different sectors such as private companies and non-government organisation to effectively address the pervasive nature of cyber threats in the region. This point is more significant for small states considering that they have limited material resources to develop cyber capabilities that can rival more powerful states in the region.

In evaluating the connection between cyber and conventional military, two important baselines were established. The first is that cyber capabilities are developed in concert with a broader set of information technology-driven military capabilities, as part of the RMA. The second is that a state's foreign alignment relates to its orientation towards the RMA. Building on these, the chapter demonstrated that cyber capabilities facilitate military performance through several "discursive functions" such as efficiency, intelligence, and coordination. Singapore is in a strong position to maximise the utility of cyber capabilities in military operations since it pursues a steady defence relationship with the U.S. and maintains a highly capable RMA-oriented military force. Despite its relationship with the U.S., New Zealand has limited use for cyber capabilities in military operations since the state has refused to harness the advantages of an RMA-oriented military force and it continues to limit the resources for the modernisation of the NZDF. Brunei has limited use for cyber capabilities in military operations because the state has not invested in RMA oriented modernisation and maintains one of the smallest military forces in the region. An important point that can be derived from the second section is a small state's military force must be predisposed to technological innovation before it develops the capacity for cyber operations. Despite the recognised advantages of network technologies, not all small states have the resources and the intention to build and operate a network-enabled military force.

The contribution of cyber power to the foreign policy of small states was established by exploring the different forms of cyber power and how these relate to the strategies of New Zealand, Singapore and Brunei. Compulsory cyber power has low potential for all three states mainly because these have limited resources and military capabilities relative to more powerful states with cyber capabilities in the region. Given the capacity of its military force, Singapore may find some use for compulsory cyber power but aggression in cyberspace weakens its defence strategy, which is focused on deterrence and diplomacy. Institutional cyber power has high potential for all three small states because of two reasons. First, increasing influence by engaging international institutions is already a vital foreign policy strategy of New Zealand and Singapore in advancing their interests while Brunei has just started increasing its participation in multilateral discussions regarding cybersecurity. Second, the uncertainty regarding state interactions in cyberspace makes international institutions an important instrument for building confidence and mitigating cyber conflict.

Structural cyber power reinforces the weak position small states in the international system but the experiences of New Zealand and Singapore confirm the ability of small states to adapt to and mitigate the impact of economic structures by actively transforming their networks into an instrument of economic growth rather than a source of weakness. Brunei has not achieved the technology-driven growth experienced by New Zealand and Singapore. Despite being a highly networked, Brunei's initiatives in harnessing the economic and strategic advantages of ICTs are still in progress, with the state pushing for digital transformation in the next decade. In terms of productive cyber power, both New Zealand and Singapore have been successful framing cybersecurity as a regional and global issue of concern. New Zealand well-positioned role as "norm entrepreneur" has enabled the state to contribute to key international debates and push for its agenda for cyberspace. Singapore's ambitious vision of a "Smart Nation" has generated influential discourse for innovation and cutting-edge technological advancement within the international community, strengthening Singapore's reputation as a leading financial and technology hub in the region. Brunei's demonstration of productive cyber power has low potential because of three reasons: the strategic use of cyber power remains uncertain; the drive towards a digital government is shaped by domestic factors; and the ideas and actions expressed in cyberspace may contradict or challenge the state's prevailing national philosophy. A significant point that can be teased out from the third section is that the efficacy of cyber power as a concept is limited for small states contrary to the arguments presented in the literature (Nye, 2010). This is because the ability to employ cyber power is still linked to other material factors that determine a state's capability such as strength of military forces and national CII. Since small states have limited materials resources, their ability to shape outcomes in cyberspace is also constrained as well.

In line with the explanatory framework of the study, the next chapter examines the role of strategic culture as a necessary secondary condition for the development of cyber capabilities. Strategic beliefs and practices are crucial for directing the strategy of states but this study posits that these ideas are not insufficient to compel small states to invest in cyber capabilities. Strategic culture therefore functions as a permissive condition that filters the preference of small states. Chapter 5 probes into three key analytical themes: the role of strategic culture in contributing to the network readiness; the role of strategic culture as a necessary secondary condition in developing cybersecurity strategies; and the influence of strategic culture in designating specific government agencies responsible for managing cybersecurity issues.

# Chapter 5
## Strategic Culture and Cyber Capability Development

The relative distribution of power in the Asia-Pacific Region is the primary condition that facilitates the development of cyber capabilities. This condition however, cannot account for how small states make use of networked technology to advance foreign policy interests. The inclusion of state level factors is therefore necessary to build a more inclusive and persuasive explanation for the strategic utility of these capabilities for small states. The evolution of information and communication technologies may be inevitable but the way in which states acquire strategic advantages from new technology is still influenced by ideational factors that are unique to each state (Katzenstein, 1996; Adamsky, 2010; McCarthy, 2015). In this sense, the "distinctive body of beliefs, attitudes and practices regarding use of force" or "strategic culture" (Longhurst, 2004, p. 17) is crucial in defining the utility of cyber capabilities as a foreign policy instrument for small states in the region.

The extent to which strategic culture influences foreign policy behaviour is greatly contested. The literature on the subject stretches several generations and conflicting interpretations of the concept have constrained debates from moving forward (Haglund, 2011; Bloomfield, 2012). Since resolving the divergent scholarship is beyond the scope of this research, this study builds on the work of Desch (1998), Glenn (2009) that advances collaboration between structural and cultural variables to explain the foreign policy behaviour of states. More specifically, this study follows the epiphenomenal conception of strategic culture and treats it as an intervening variable that filters the strategic preferences of states within a geopolitical environment shaped by the relative distribution of power.

This chapter treats strategic culture as an important factor that affects the development of cyber capabilities in small states. It applies the second part of the theoretical framework mentioned in Chapter 2, where strategic culture is considered a necessary secondary condition that has some influence on the foreign policy preferences of small states, particularly the development of cyber capabilities. Strategic beliefs and practices are considered as a secondary condition because these functions as a filtering mechanism that shapes the responses of small states to the structural conditions in the Asia-Pacific Region. This framework creates a dynamic whereby the strategic preferences of small states to develop cyber capabilities are primarily driven by the relative distribution of power but how these states use the capabilities are shaped by their strategic beliefs and practices. The following questions are explored to facilitate the comparison between the three case studies in the chapter:

1. How does strategic culture relate to the network readiness of small states?
2. What is the role of strategic culture as a necessary condition to the development of cybersecurity strategies in small states?
3. What is the contribution of strategic culture in assigning the government agencies responsible for cybersecurity in small states?

The remainder of this section explores the prevailing strategic culture of the small states and develops a new concept to clarify the role of technology in supplementing the respective strategic cultures of small states. The second section tackles the first question by examining the role of strategic culture in contributing to the network readiness of the selected states. Network readiness is a useful measurement because it is a reasonable indicator of states' interest and investment in digital technologies. The third section considers the second question by establishing the role of strategic culture as a necessary secondary condition in developing cybersecurity strategies. The fourth addresses the third question by examining influence of strategic culture in designating specific government agencies responsible for managing cybersecurity issues. The assignment of responsible agencies is important because these practices suggest the type of approach that a state intends to pursue in securing cyberspace. A state's approach to cybersecurity is an indicator of preference because these actions reflect the strategic beliefs and practices regarding the use of networked technology. The last section recapitulates the main themes of the chapter and connects the findings with the overall framework of the study.

*Prevailing strategic culture*

The strategic culture of the small states have been the subject of previous inquiries, however a brief review of the existing strategic beliefs and practices of New Zealand, Singapore, and Brunei is useful to strengthen analysis of the chapter. While International Relations scholars contend that strategic culture changes over time, this subsection surveys the prevailing strategic culture that influences the foreign and security policies of each of the three small states since the start of the twenty first century (Lantis, 2002; McCraw, 2011; Bloomfield, 2012). This period is notable for two reasons. First, the commercialisation of the Internet emerged towards the end of the twentieth century thereby enabling states to harness advantages of connectivity and develop new capabilities for cyberspace (Naughton, 2016). Second, this is also significant because first movers in the area of military technology such as China and the U.S. started developing full-scale cyber capabilities during the late 1990s (Healey, 2013).

New Zealand's prevailing strategic culture can be characterised as "anti-militarist", a belief that is demonstrated by the state's responses during two foreign policy dilemmas. The first dilemma was the dispute with the U.S. over nuclear ship visits in 1985 where the state denied the USS Buchanan port of entry because the military vessel could not confirm that it was nuclear-free. The incident escalated into a crisis because New Zealand's nuclear-free policy prevailed over an enduring defence arrangement with a great power. This move compelled the U.S. to suspend its security guarantee to New Zealand under the trilateral ANZUS Treaty (Catalintac, 2010). The state's clear preference for enforcing a nuclear-weapons-free zone within its territory is consistent with its strategic culture because the agenda of nuclear disarmament lies at the core of New Zealand's anti-militarist belief.

The second dilemma was New Zealand's refusal to participate in the U.S.-led invasion of Iraq in 2003 because the action was not officially sanctioned by the United Nations. New Zealand's preference not to participate in military action is influenced by its strategic culture because it chose to adhere to its core belief of respecting international laws and norms rather than supporting the U.S. and potentially revive its damaged defence relationship. This case is again consistent with the state's anti-militarist outlook that favours pursuing diplomacy and negotiation through international institutions more than using military force in resolving conflicts (McCraw, 2011).

The anti-militarist belief continues to be the central idea of New Zealand's strategic culture in the twenty first century. There are two indications of this assertion. The first is the constantly low defence expenditure of state, allocating around 1.2% (regional average is 1.8%) of its GDP for national defence from 2000 to 2016 (Stockholm International Peace Research Institute [SIPRI], 2016).[13] Extensive resources are necessary to enable the New Zealand Defence Force to adapt to the evolving strategic environment therefore sustained limited defence spending suggests that no change in strategic outlook.

Another example is the document *Strategic Intentions 2015-2019* produced by the Ministry of Foreign Affairs and Trade which underscores the significance of international institutions through New Zealand's membership in the United Nations Security Council. This effort is a reflection of the state's current strategic culture because it highlights the state's core strategy of pursuing diplomacy and negotiation through international institutions such as the United Nations (Ministry of Foreign Affairs and Trade, 2015, p. 8). While small states typically engage with international institutions to enhance their influence and bargaining power, New Zealand is one of the more active states particularly in the areas of nuclear non-proliferation, international law, and more recently, cybersecurity (Buchanan, 2010; Burton, 2013).

Singapore's prevailing strategic culture can be characterised as "insecure" and shaped by a "siege mentality" (i.e. defensive or paranoid) (Tan, 2012). These cultural traits were developed during the state's difficult path towards establishing sovereignty and national identity after its declaration of independence from Malaysia in 1965. Singapore's strategic culture remains intact despite the absence of any military threat by an external power. This insecurity can be confirmed by evaluating three indicators. The first is the state's defence expenditure. Singapore consistently spends a remarkable amount of resources on national defence, assigning around 3.9% (regional average is 1.8%) of its GDP from 2000 to 2016 (SIPRI, 2016). As discussed previously, Singapore believes that maintaining a highly capable, technological advanced military force is necessary to mitigate its inherent material limitations and advance its national interests in a competitive geopolitical environment.

The second is the state's geography. Singapore is located adjacent to Malaysia and Indonesia, both of which contribute to the state's insecurity because of previous disputes as well as tensions over natural resources such as water, air quality, and airspace (Heng, 2013; Heilmann, 2015). In response, the state continues to be suspicious of the intentions and the capabilities of its neighbours,

[13] North Korea, Turkmenistan, and Uzbekistan were excluded from the estimate because of the lack of data on their respective military expenditures.

reinforcing its strategic culture and invariably its foreign and security policies. The third is the state's foreign policy strategy. Singapore pursues a hedging strategy to ensure that it attains its national interests while preserving the regional balance of power (Huxley, 2006). This strategy calls for active engagement with great powers while limiting political attachments to any state. This move is designed to enhance the state's strategic options in different foreign policy areas but it also reflects the Singapore strategic culture because it lessens the tendency to develop alignments with a powerful state through trade and defence agreements. Indeed, hedging allows Singapore to pursue its foreign policy interests in line with its strategic culture because the strategy emphasises self-reliance more than dependence on other states.

Brunei's strategic culture can be characterised as "conditioned" because the beliefs and practices of the state relating to use of force are anchored on the *Melayu Islam Beraja* (MIB) or Malay Islamic Monarchy ideology and stringently implemented by Sultan Hassanal Bolkiah. The state's beliefs and practices are "conditioned" because the MIB ideology functions as a permissive or restrictive condition that affects how Brunei responds to foreign policy issues such as territorial disputes and great power rivalry. In this context, the Sultan through the MIB ideology, dictates the state's core strategic interests: preserve the monarchy; maintain a stable regional environment; and develop sufficient defence capabilities to defend the state's sovereignty and territorial claims (Walsh, 2011). This characterisation of Brunei's strategic culture can be observed through three implications.

The first implication is Brunei's focus on internal security despite its proximity to previous adversaries. This practice is driven by the Sultan's continued sense of insecurity and vulnerability attributed to a decisive armed insurrection that involved the Brunei People's Party (linked to Malaysia) and North Kalimantan National Army (supported by Indonesia) in 1962 (Majid, 2007). Following this experience, the Royal Brunei Armed Forces is configured to address internal security threats as reflected in the small size of its military force with no reserve forces or mandatory military service (Cheng-Chwee and Welsh, 2008, pp. 63-65).

The second is the state's continued requests for the presence of British Armed Forces within its territory. Brunei ceased to be a protectorate of the U.K.

in 1984 but it continues to enjoy the security assistance of the U.K. through the deployment of a Royal Gurkha Riffles Division, an Army Air Corps Flight of Bell 212 as well as British Army's Jungle Warfare Division. This continuous scheme not only reflects enduring and deep diplomatic ties between Brunei and the U.K. but also a carefully crafted military strategy of countering potential rebellion through external military assistance. In this regard, the continued presence of British Armed Forces is consistent with Brunei's strategic culture because the arrangement ultimately benefits the Sultan who is the main influence of the state's strategic preferences.

The third implication is the state's low-profile approach to the territorial dispute in the South China Sea. The approach is low profile because Brunei's response to tension over the disputed islands has been measured, avoiding any bickering or display of aggression towards other states. Moreover, while the state claims Louisa Reef, an island located within its Exclusive Economic Zone, it does not station any military forces on the territory unlike other claimant states. The main reason behind this approach is to avoid any tension with China, which is one of Brunei's top trading partners but more significantly a long-time supporter of the Sultanate of Brunei. In fact, bilateral relations between the two states date as far back as the Han Dynasty, with the tomb of Sultan Abdul Majid Hassan (second sultan of Brunei) being erected in Nanjing, China during the Ming Dynasty in the early fifteenth century. In line with this, the Sultan's preference for preserving its enduring relationship China while asserting the state's claim in the South China Sea has influenced Brunei to adopt a low-key, non-confrontational approach to dispute management (Oishi, 2015, pp. 70-71).

### *Technological dimension of strategic culture*

The preceding section presented the prevailing strategic beliefs and practices of the three small states by surveying the historical experiences as well as the geopolitical conditions affecting the states. Since the focus is on cyber capability development, this subsection builds on these narratives by expanding on the technological dimension of strategic culture. The objective therefore is to contribute to the literature by developing a concept that captures the tendency of small states to depend on digital technology to enhance their strategic options and survive in a contentious geopolitical environment.

The interplay between culture and technology in shaping strategic preferences of great powers such as China, Russia and the U.S. have been examined in previous studies but the implications for small states is currently understudied (cf. Snyder, 1977; Johnston, 1996; Mahnken, 2008; Harris, 2009; Adamsky, 2010). The *term* "technology-oriented" is presented to clarify the role of technology in the context of prevailing strategic cultures of selected small states. In developing this concept, this section draws on the work of Gerring (2012, 116) that identifies four basic elements of an empirical concept: *term, phenomena, attributes,* and *indicators*. These elements will be used as a framework for concept formation in this section.

The *phenomena* being explained is the concept of a technology-oriented strategic culture and how this relates to the foreign policy preferences of small states. Technology-oriented is defined as the preference of small states for using digital technologies to compensate for their material limitations in advancing foreign policy interests. This concept supplements the prevailing strategic culture because it describes the interaction between culture and technology in the relation to the foreign policy preferences of small states. Since the strategic use of cyberspace is relatively new, developing a concept that emphasises the technological dimension of strategic culture is necessary to strengthen current knowledge regarding cyber phenomena.

The idea of technology-oriented is informed by the theory of the network society that advances a "society where the key social structures and activities are organized around electronically processed information networks" (Castells, 2001). A societal perspective is useful to consider in concept development because ICTs affect both civilian and military sectors, supporting all processes and infrastructures within a state. In this sense, the network society is an appropriate theory to draw on because it is the "most sophisticated" theoretical construct available that accounts for changes social structures in the twenty first century (Garnham, 2004, 165). While the network society does not directly consider the emergence of cyber capabilities in strategic affairs, the theory contributes three fundamental *attributes* that are useful for building the concept: information driven, pervasive technologies, and network logic.

Information driven is the first attribute that defines a technology-oriented strategic culture. Information is arguably the most valuable resource in the twenty first century and a key feature that directs the strategies of states driven by a technology-oriented strategic culture. Since information is central to business and government transactions, small states with limited material resources and critical, information infrastructures (CII) harness information with the objective of gaining strategic advantages over adversaries. Information is an essential component of the concept because it is the "raw material" that characterises the technological orientation of small states (Castells, 2000/2010, p. 70).

The pervasiveness of new technologies is a second attribute that describes a technology-oriented strategic culture. This refers to the presence of ICTs in all aspects of human activity that shapes "all processes of our individual and collective existence" (Castells, 2000/2010, p. 70). This is an important attribute because new technologies are a prerequisite for boosting information exchange and building networks within and among states. The ubiquity of technology not only allows states to provide necessary basic services but also enables states to manage change and ambiguity in international politics (Bjola and Holmes, 2015).

The third attribute is the networking logic that drives the basic aspects of a state's existence such as government processes, modes of production, and information exchange in the Information Age. Networks or "a set of interconnected nodes" are well suited to adapt to increasing complexity and interaction at the state level and more importantly interactions between states in cyberspace (Castells, 2001, p. 15). More specifically, networks accelerate the dissemination of information about any issue or event regardless of accuracy that can shape foreign policy debates, develop coordinated action between states and achieve successful policy outcomes (Westcott, 2008).

The first three attributes are adopted from the fundamental characteristics of the network society but since the concept developed here is focused on strategic affairs, two additional attributes – technology in external affairs and social engagement through technology – are presented to sharpen the distinctiveness of the concept. Taken collectively, these five attributes illuminate the concept of a technology-oriented strategic culture, a necessary secondary condition that filters how small states respond to the relative distribution of power in relation to development of cyber capabilities in small states. The role of strategic culture as a secondary condition and its interplay with the power imbalance in the region are discussed in detail in the third section of this chapter.

The fourth attribute is the role of technology in managing the external affairs of a state. This refers to how states use ICTs to respond to security dilemmas and foreign policy issues. Technology facilitates different dimensions of state interactions from diplomacy and trade to espionage and conflict hence states are influenced to utilise ICTs to generate more economic opportunities, promote efficiency in government transactions and enables rapid access to vital information (Sachs, 2000, p. 6). The use of technology is particularly significant for small states given the intrinsic limitations of these states in terms of material resources and capacity to influence relative to other states in the Asia-Pacific Region.

Social engagement through technology is the fifth and last attribute. This refers to the level of public awareness on cyber issues and connectivity of the population within small states (Feakin et al. 2016, p. 10). Strategic culture is defined by collective beliefs and practices of the people within the state. In this sense, a strong cyber public awareness campaign is essential to a state oriented towards the use of networked technology-. In addition, better public understanding of cyber issues should be complimented by reliable and secure network connectivity that enables social engagement through cyberspace. Both elements are indicative of the influence of a technology-oriented strategic culture of small states.

There are three *indicators* or observable implications used to characterise the technology-oriented strategic culture based on empirical evidence. The first, network readiness, refers to measures of how well a state is "using information and communications technologies to boost competitiveness and well-being" (World Economic Forum, 2016). This indicator is evaluated through the NRI published annually by the WEF since 2001. The second, policy discourse, concerns the relevance of cybersecurity as an issue in the national security discourse of selected states. This is observed through an assessment of the national security documents of selected states (i.e. national security strategies, defence white papers). The third indicator is the role or contribution of government security agencies in the cybersecurity strategies of the selected states. This is discerned through a review of the cybersecurity strategies and relevant official documents such as national technology plans of selected states. These indicators are substantiated and contextualised in the succeeding sections of the chapter.

## Strategic culture and network readiness

The interest of small states to develop a network society through reliable CII as well as elaborate networks that enable effective government services, including military capabilities, is influenced by their respective collective beliefs and practices. Indeed, the relevance of strategic culture in developing and utilising networked technologies for strategic purposes has been discussed in previous studies. For instance, Adamsky (2010, p. 1) contends that American, Soviet, and Israeli strategic culture can account for their varying approaches to military technological innovation. Manhken (2009) offers a similar view by arguing that that strategic culture plays a significant role in shaping American's preference for advanced technology: "Reliance on advanced technology has been a central pillar of the American way of war, at least since World War II. No nation in recent history has placed greater emphasis upon the role of technology in planning and waging war than the United States" (p. 5). Raska's (2011, p. 8) work is the most relevant to the study because it postulates that strategic culture is one of "at least three underlying drivers that may support and accelerate" RMA diffusion in small states.

While these studies confirm the link between strategic culture and technology they do not consider the implications for the development of cyber capabilities. This study builds on these previous works by exploring the connection of strategic culture on the emergence of cyber capabilities. Since network readiness is the most comprehensive assessment of how states derive competitive advantages from ICTs (Kirkman, et al., 2002), it is an appropriate indicator that can signify a state's technology orientation as it relates to strategic culture.

This section develops the connection between culture and technology by relating the sources of strategic culture with the network readiness of Singapore, New Zealand, and Brunei. Studies by Booth and Trood (1999) and Lantis and Howlett (2007) suggest that there are several sources of strategic culture encompassing both material and ideational factors. This study narrows these sources to two by drawing on state-specific literature that indicates that *geography* (cf. Chwee Kuik and Welsh, 2005; Johnston, 1997; Heng, 2013) and *natural resources* (cf. Emmers, 2012; Mathews and Yan, 2007; Burton, 2013) are prominent sources of strategic culture for all states in the Region. Brunei however, has been lagging behind in terms network readiness because of the restrictions prescribed by its national ideology, the MIB (Tisdell, 1998, pp. 403-404). In this sense, the study uses the identified sources as an organising framework to compare the three cases and explain how these affect the network readiness of small states.

*Geography*

Geographic location is a key source of beliefs and practices for small states because it influences states' strategic calculations and responses to their strategic environment. Geography has proven to be an instrumental source of conflict and cooperation between states in the Asia-Pacific (Ball, 1993; Lantis, 2014; Mahnken and Blumenthal, 2014). Since powerful states such as China and the U.S. use their considerable military power to advance their interests, small states situated in the region are vulnerable and insecure of more powerful neighbours given the prospects of conflict escalation due to territorial disputes, historical animosities, and great power rivalry (Tan, 2014; Holslag, 2015; Croker, 2015). Small states have therefore relied on technology to manage uncertainty and develop more innovative national security strategies that can enable them to thrive in the Asia-Pacific.

Geography is a crucial source of strategic culture for New Zealand. The state is not confronted by any external threats from adversaries, a predicament that can be attributed to its distinctive geographic location. Indeed, the state's anti-militarist strategic culture is influenced by the absence of external threats due to its geographic isolation from other states in the region. This benign strategic environment continues to be a strong rationale for maintaining a small military force that is focused on maritime security and military operations other than war (Ayson, 2016).

However, the state's geographic isolation and small territory is also a source of weakness because it limits the capacity of the state to generate national income thereby affecting its capacity to enhance its defence forces. This challenge has been addressed through active investment and use of technology for different functions of government including defence and military organisations. New Zealand's high network readiness level (20 out of 148 states) reflects the interest of the state to compensate for its geographical limitations by using technology to increase its defence readiness and economic growth (Bilbao-Osorio, et al., 2014). In this regard, the link between geography and network readiness is manifested in New Zealand's case in two ways.

The first is New Zealand's intensive efforts to further upgrade its Internet connectivity through its Ultra-Fast Broadband programme and Rural Broadband Initiative. More specifically, the government is investing in $2 billion to provide 99% of New Zealanders with access to speeds of at least 50 Mbps by 2025 (Ministry of Business, Innovation and Employment [MBIE], 2017).[14] This initiative suggests a link between geography and network readiness because increased connectivity contributes to stronger networks that enable New Zealand to transcend the barriers of geographic isolation in critical areas of trade and investment as well as and defence readiness (Muller, et al., 2016, 10, New Zealand Defence Force [NZDF], 2012, p. 5). A second is the sustained development of the New Zealand's technology sector. The steady growth of the state's technology sector can be partially attributed to the government's efforts in promoting the significance of ICTs in diminishing the geographic limitations of New Zealand since the start of the twenty first century (Clark, 2000; Keys, 2016). To be sure, recent government reports indicate a 100% growth in ICT services and software exports from 2008 to 2014, with the technology sector contributing 8% of the state's gross domestic product (GDP) in 2015. The sustained growth and innovation in the technology sector is another indicator of the connection between geography and network readiness since the move towards a "digital nation" has been compelled by the small size and relative isolation of New Zealand in the Asia-Pacific (Muller, et al., 2016, p. 10).

Singapore's geography is also a significant source that has shaped its "insecure" strategic culture. While the state has not been subjected to any external threats in the past fifteen years, Singapore's insecurity continues to affect its strategic posture because of its geography: beside previous rivals Malaysia and Indonesia and relatively close to territorial disputes in the South China Sea. Moreover, the state's lack of strategic depth can also be attributed to its very small land area that makes it more vulnerable to a military invasion by more powerful

[14] New Zealand's Internet speed was recorded at 14.7 Mbps in 2017. The global average in 2017 was 7.2 Mbps (Belson, 2017, p. 12).

states. Singapore's geographic location is very different from New Zealand however, both states derive a sense of vulnerability from their natural geography that has contributed to their interest in building a networked society (Heng, 2013; Burton, 2013).

This sense of geographic vulnerability has compelled the state to achieve a "technological edge" over other states in the Asia-Pacific (Matthews and Yan, 2007). Indeed, Singapore's status as one of the highest in network readiness (2 out of 148 states) reflects the interest of the state to compensate for its geographic vulnerability by using technology to strengthen its defensive posture as well as to maintain high levels of economic growth (Bilbao-Osorio, et al., 2014). In this context, the connection between geography and network readiness is reflected in two crucial initiatives: the Smart Nation Platform (SNP) and the formation of specific government agencies for cybersecurity.

Singapore's SNP is a national effort to support a better quality of life through extensive and systematic use of technology to empower all members of Singaporean society and allow the state to compete with the global leaders in technology and innovation (Lee, 2014). The objective of the SNP is to enable "pervasive connectivity, better situational awareness through data collection, and efficient sharing of collected sensor data" across the entire state (Singapore InfoComm Development Authority, [IDA], 2014). This initiative is a strong indicator of the role of geography in enhancing high network readiness because Singapore's drive to maintain the technological advantage over other states is informed by the belief that it is vulnerable to adversaries because of its lack of strategic depth and geographic location.

Another initiative is the development of government agencies focused on cybersecurity. Singapore's efforts in securing computer networks evolved from the creation of the National Computer Board (NCB) in 1981 to the formation of an InfoComm Development Authority (IDA) in 1999, and more recently the establishment of the Cyber Security Agency in 2016. While spanning several decades, these agencies were primarily created to manage and regulate Singapore's constant investment in new technologies necessary to compensate for its intrinsic geographical vulnerabilities. The formation of government agencies relates to the linkage between geography and network readiness because the agencies were established in response to Singapore's sustained investment in advanced technology. In this sense, maintaining a high level of network readiness is critical for Singapore to leverage technology as a source of strength that mitigates vulnerabilities associated with its geographic location.

Brunei shares some similarities with New Zealand and Singapore since the state also has limited land area and existing coastlines that are consequential for its territorial defence. The state's geographic location is also analogous to Singapore because it is located along the South China Sea, a contentious area of the Asia-Pacific. In this regard, Brunei derives some vulnerability from its geographical position since powerful neighbours, Malaysia and Indonesia, previously attempted to undermine the sovereignty of the state (Chwee Kuik and Welsh, 2005). Even if the state is not confronted by any existential threat, it continues to be in a fragile strategic position because of its small size and lack of geographical barriers to enhance its territorial defences.

In contrast to New Zealand and Singapore however, Brunei's geographic constraints have not been a persuasive factor in influencing the state to use ICTs in achieving its security and foreign policy objectives. This is reflected in the fact that Brunei's network readiness is lower than New Zealand and Singapore (45 out of 148 states), suggesting that the state's orientation towards the investment in digital technologies is different.  Two implications can be derived from Brunei's case. First, Brunei recognises that technology is crucial in managing its geographic constraints but the state's prevailing beliefs and practices regarding ICTs challenge the idea of widespread technological innovation. This point is explored further in the next section. Second, the clash between the use of digital technologies and Brunei's prevailing strategic culture impedes the development of cyber capabilities because the employment of these capabilities requires progressive investments in digital infrastructure as well as human resources. Indeed, exploiting and defending computer networks are multi-faceted processes that require continuous innovation and adaptation to become effective (Buchanan, 2016, pp. 31-72).

The preceding section established the significance of geography as source of strategic culture that influences the technology orientation of small states. Two key implications can be drawn from the previous section. The first is that geography remains a fundamental element that affects strategic culture despite the pervasiveness of network-technology. Geographic limitations are critical in enhancing state dependence on network-technologies despite the clear differences in New Zealand's "anti-militarist" and Singapore's "insecure" strategic cultures. While geography does not seem to be as influential in Brunei's case, the lack of external threats, which is still can be attributed to geography, allows the state to limit its engagement with network-technologies and downplay the need to develop strong cyber capabilities. The second is that a benign strategic environment is not necessarily advantageous for small states because it breeds complacency regarding external threats thereby affecting the rationale for strengthening military forces (McCraw, 2008). This is evident in the case of Brunei and New Zealand considering that these states need to adjust to the prevalence of cyber threats that are linked to interstate territorial and political disputes but are not constrained by geographic boundaries.

### *Natural resources*

Natural resources are another main source of strategic culture for small states. Indeed, one of the defining characteristics of "smallness" is the limited national resources of states', which inevitably constrain their military capabilities (Handel, 1981; Elman, 1995). Natural resources such as petroleum, minerals, and natural gases are fundamental sources of state power and central to state survival in the Asia-Pacific. The strategic importance of material resources is clearly reflected in the fact that states with extensive natural resources such as Australia, China, Japan, and the U.S. tend to maintain the most capable military forces as well as hold considerable political influence among states in the Region (Dibb, 1997; Tan, 2014; Ayson, 2015).

Small states are therefore compelled to adjust to this reality by employing different foreign policy strategies that centre on dependence or self-reliance (Hey et al., 2003; Bailes, et al., 2016; Panke, 2017). In both cases, the objective of small states is to increase their strategic options and mitigate the vulnerabilities caused by limited resources. The investment in networked technology and high network readiness supplements the different strategies used by small states because computers and networks facilitate the flow of information vital to all levels of state interaction.

Natural resources are a notable source of strategic culture for New Zealand. This is because the state depends on its own food and agriculture industry as the primary source of national income and its main trade export in the Region. More specifically, New Zealand specialises in exporting concentrated milk (13%), assorted meat (12.2%), butter (4.5%), and wood (4.5%) (Observatory of Economic Complexity [OEC], 2015). While these natural resources have managed to sustain the state's requirements, the continued use of these resources is no longer sustainable with some resources such as water approaching environmental limits or "the boundary beyond which exploitation of a natural resource will have significant deleterious effect" (Wentworth, 2010, p. 1; Girouard, et al., 2016, p. 12). Moreover, the extensive agricultural activities in New Zealand over the past years have increased greenhouse gas emissions and threatened biodiversity thereby giving more reason for the state to rethink its economic strategy (Girouard, et al., 2016). The fundamental challenge of limited natural resources is a key factor that affects the state's ability to comprehensively upgrade the capabilities of the New Zealand Defence Force (NZDF), which needs to constantly adapt to the changing geopolitical environment in the Asia-Pacific (New Zealand Ministry of Defence, 2016). In this context, the connection between natural resources and network readiness can be observed in New Zealand's case in two specific initiatives: technology as a supplement to natural resources and technology as an enabler of other industries.

New Zealand's keen interest in strengthening its digital environment by investing in CII and maintaining a high-level of network readiness is motivated by the projected limitations of its natural resources, the state's primary source of income and competitive advantage in terms of trade. Developing a robust technology sector as an alternative source of income is crucial for New Zealand to prevent environmental degradation as well as generate more resources essential to modernise its military force as a response to geopolitical challenges in the Asia-Pacific. The importance of generating sufficient resources to enhance the "flexibility and depth of capability" of the NZDF is clearly articulated in the *Defence White Paper 2016* which argues for spending "$20 billion in the next 15 years" (New Zealand Ministry of Defence, 2016, p. 7). This defence budget can be sustained with strong contributions from technology sector given that the sector can generate as much as USD 16.2 billion or around 8% of New Zealand's GDP (Muller, et al., 2016, p. 12). In this regard, solely depending on natural resources is no longer enough to sustain New Zealand's technological innovation, particularly a high level of network readiness to support economic growth and national defence.

Another connection between natural resources and network readiness can be observed from New Zealand's investment in technology to compensate for the limitations of natural resources. While natural resources remain the primary source of income and competitive advantage, these elements were not necessarily designed to enable the productivity of other industries. Information and communication technologies however are different because these can be customised to support other key industries such as manufacturing, constitutes 10% of New Zealand's GDP in 2015 (New Zealand Treasury, 2016, p. 20). In fact, the New Zealand Technology Industry Association reports that innovation of the technology sector effectively supports the growth of the manufacturing and retail industries by reducing the cost of doing business and exposing local firms to global markets. More specifically, New Zealand's high network readiness level has been advantageous for both retail and manufacturing sectors by facilitating "the connection of goods, machines, suppliers and consumers to each other" (Muller, et al., 2016, pp. 61-62). In essence, the limitations of natural resources have motivated New Zealand to invest in ICTs to increase the productivity of other key industries and eventually contribute to economic growth.

In comparison to New Zealand, the lack of rather than the existence of natural resources is a prominent source of strategic culture that influenced the high network readiness level of Singapore. In fact, the state does not possess any significant natural resources and its main exports and source of national income are technology-oriented: integrated circuits (17%), refined petroleum (15%), computers (3.8%), and Oxygen Amino Compounds (2.7%) (OEC, 2015). Whereas New Zealand's turn to technology was motivated by unsustainable natural resources, Singapore's interest in technology was naturally influenced by the idea that advanced technology can make up for the absence of natural resources within its small territory (Chong, 2006). Singapore has certainly gained from the economic advantages facilitated by ICTs, however, its highly networked status has made its computers and networks vulnerable to exploitation and sabotage. Consequently, the state's natural reliance on technology-oriented trade and services has become vulnerability because these steady sources of income can experience serious disruptions by any perception of computer system failure or network security breach (Ho, 2009, p. 5).

The specific manifestation of the link between natural resources and network readiness can be discerned in the way in which Singapore has developed since its independence from Malaysia in 1965. To be sure the state's "founding fathers" emphasised the potential of cutting edge technology as a key driver for economic growth, national defence, and overall progress for a small state like Singapore. For instance, Singapore's first Prime Minister Lee Kuan Yew (1999) stated: "…People must stay abreast of the state-of-the-art technology, but must never lose their core values. Science and technology are decisive in determining future progress." Singapore's first Minister for Defence Goh Keng Swee argued similarly, maintaining that science and technology were essential for national development of a small state and a force multiplier for the SAF (Ho, 2009; Loo, 2012). Lastly, Singapore's first Minister for Foreign Affairs S. Rajaratnam (1972) envisioned that Singapore could transform into a "Global City" through the investment in modern technology that linked different states together and facilitated economic interdependence. Following these ideas, maintaining the technological edge to counteract the absence in natural resources has been a guiding doctrine for Singaporean leaders since its foundation as a state.

As with New Zealand, natural resources are a vital source of strategic culture for Brunei. The state has systematically exploited its natural reserves and is highly dependent on the extraction of hydrocarbons, particularly petroleum gas (55%) and crude petroleum (38%) as a primary source of exports to generate national income. However, like New Zealand, Brunei's reliance on natural resources is not sustainable because of two reasons. The first is that hydrocarbons are non-renewable meaning these resources do not form within a short period. This is a problem because it is likely that Brunei's hydrocarbon reserves will be depleted by 2040 thereby significantly diminishing the state's national income if not sufficiently augmented by other sources of income (Duraman, et al. 1998). The second is that sale of hydrocarbons is not sustainable because the exploration and extraction costs rise over time. This is a challenge because as exploration and extraction of resources become more difficult, the costs to undertake these operations increases over time therefore making the sale of oil and gas unprofitable unless the market prices increase sufficiently to cover the costs (Lawrey, 2010, p. 16).

Despite these limitations, Brunei has yet to turn to technology as an alternative source of national income unlike New Zealand and Singapore. There are efforts to enhance network readiness across all sectors but the government has been cautious in implementing a full-scale digital transformation because of the potential of technology, specifically the Internet to disrupt the status quo as prescribed in the official state ideology, the MIB. While geography and natural resources are important sources of strategic culture for small states, national ideology is a third and coequal source of strategic culture that defines the difference between Brunei and the other two states. National ideology is equally significant for Brunei because it conditions how the state responds to geopolitical pressures related to geography and natural resources. In this regard, there is no clear connection between natural resources and network readiness in Brunei's case because the state's specific political preference is an intervening factor that defines the different between the three cases.

The previous discussion established the relevance of natural resources as source of strategic culture that contributes to the technology orientation of small states. Two key implications can be drawn from the comparison between the three cases. First, natural resources are a fundamental source of strategic culture that affects the technology orientation of small states. For instance, New Zealand's depleting resources has compelled it to develop a digital economy to supplement its national income. Strong dependence on network-technologies however requires the capacity to protect computer systems and networks. In this context, New Zealand has developed defensive cyber capabilities that are consistent with its "anti-militarist" beliefs and practices. Singapore's lack of natural resources has forced the state to turn to technology as a main source for generating national income. The state's enduring engagement with network technologies has influenced its strong capacity for cyber operations. In contrast with New Zealand, Singapore has developed more elaborate cyber capabilities in line with its culture of insecurity. Brunei on the other hand, is reluctant to change the status quo in terms of its dependence on depleting natural resources and level of engagement with network technologies. The state's over reliance on oil and gas has left it vulnerable to resource depletion as well as cyber intrusions that can disrupt its economy and society as well. This predicament can be attributed its "conditioned" strategic culture that influences the state to resist change.

*National ideology as a differentiating factor*

Brunei's protracted investment in technology and its inevitably lower levels of network readiness can be attributed to its cohesive national ideology. Before analysing the influence of national ideology on the state's strategic culture, it is necessary to clarify the relationship between national ideology and strategic culture. The concept of national ideology or a "coherent set of ideas that provides a basis for organized political action, whether this is intended to preserve, modify or overthrow the existing system of power relationships" (Heywood, 2014, p. 28) is similar to strategic culture because both prescribe ideas that constrain or compel different type of actions. Whereas the literature on strategic studies identifies national ideology as a potential source of strategic culture (Lantis and Howett, 2013, p. 88), this study argues that the MIB or Malay Islamic Monarchy encompasses the strategic culture of Brunei because these prescribed ideas are permeated the within all levels of government and society of the state thereby conditioning its preferences towards the use of force. In other words, Brunei's national ideology *is* also its strategic culture. There are two observations that reinforce this assertion. First, upholding the national ideology is a core mission of the RBAF therefore the strategic preferences of the state must be consistent with the ideas prescribed by the MIB (Brunei Ministry of Defence, 2011). Second, although the RBAF engages with different strategic beliefs and practices given its close cooperation with the UK and the U.S., these ideas are always secondary to the national ideology (Brunei Ministry of Defence, 2004, 2015; Brunei Information Department, 2016).

The MIB was introduced as the ruling ideology of Sultan Hassanal Bolkiah during the period leading up to Brunei's independence from the UK in 1984. Brunei's ideologues contend that ideology reflects the "ancient reality" of a community devoted to the monarchy by ties of loyalty as well as the Sultan's expression of religious solidarity as a "caring Caliph" of outstanding virtue (Kernshaw, 2001, p. 124). Previous studies however suggest that the MIB ideology is more than a cultural and religious symbol, it is the primary basis for the Sultan's continued legitimacy particularly in three strategic areas of society: (i) politics (i.e. regime legitimacy and succession); (ii) religion (i.e. Islam as the national religion); (iii) ethnicity (i.e. rights and privileges of the Malay community) (Horton, 1994; Chachavalpongpun, 2013; Talib, 2013).

A national ideology is therefore decisive for an absolute monarchy to sustain its power and influence through the control of information networks. Enhancing network readiness however, presents a serious dilemma for the monarchy because while Brunei has one of the highest Internet penetration rates in the region, the state's engagement with ICTs continues to be restrained at best.

This claim can be substantiated in four crucial aspects of Brunei's society. The first is economic: the state continues to be reluctant to diversify its economy despite the diminishing profitability of its natural resources over time (Tisdell, 1998; Blomqvist, 1998). In the absence of other natural resources, technology can be a feasible alternative source of national income for the state like New Zealand and Singapore's experience. The second is political: Sultan Hassanal Bolkiah is disconcerted about the impact of network technologies on Brunei's society because of its potential to facilitate the beliefs and practices that can challenge the national ideology of Malay Islamic Monarchy. He contends that MIB ideology is the state's "strong and effective firewall" to "overcome a variety of issues and challenges as well as changes that come with globalisation" (BPMO, 2014).

The third is military: the state has just started to invest in networked platforms and systems to enhance the capabilities of the RBAF. Brunei maintained strong ties with powerful states such as U.S. and UK since its independence in 1984 but the state's military modernisation just started recently, particularly its efforts to strengthen its military's capacity for integrated command-and-control systems and purchase of larger weapon systems like naval vessels (Roberts and Cook, 2016). Indeed, Brunei continues to maintain a small military force and has just started implementing is framework for enhancing the capabilities of the Ministry of Defence and RBAF in 2016 (Brunei Ministry of Defence, 2016). The fourth is societal: public awareness and debates regarding cyber issues are limited due to strong state regulation of media outlets as well as online forums (Feakin, et al., 2016). Whereas television, radio and the Internet is widely accessible, intelligence and law enforcement agencies monitor online material, and domestic newspapers, radio stations, and television programmes that are linked to the government to ensure that there is no subversive content that challenges the national ideology of the state (Croissant and Lorenz, 2018, pp. 27-28). This is vital because limitations to Internet content and online exchanges contradict the objective of achieving high levels of network readiness.

Following these observations, the dilemma confronting the monarchy is further compounded by the fact that ICTs facilitate new beliefs and practices that can mobilise action and challenge the status quo of the state. Democratic revolutions enabled by technology are well documented in the twenty-first century. Recent studies highlight the prominent role of digital technologies in facilitating paths or barriers to democratic transition in states with large Muslim communities such as Tunisia, Iran, Egypt, and Libya (e.g. Eckielman and Anderson, 2003; Howard, 2010; Howard and Hussain, 2013). Exploring the impact of technology on Brunei's political landscape is beyond the scope of this study but what is crucial is the state's strategic culture or the driving force behind its disinclination towards enhancing its network readiness and harnessing the advantages of a network society.

Brunei's experience highlights the significance of strategic culture as a crucial state level factor that supplements the relative distribution of power in influencing the development of cyber capabilities in small states. These findings however, are not generalisable because they are only derived from a few cases. In this context, the study can only support two inferences postulated in the literature on strategy and foreign policy. First, structural conditions alone are insufficient to change the technology orientation of small states. Second, strategic culture is a relevant conditioning factor that filters the foreign policy preferences of states.

## Strategic culture as a secondary condition

Foreign policies are shaped by collective beliefs and practices of a community, reflected in the actions taken to respond to security challenges confronting the state. Cybersecurity has evolved into a complex foreign policy issue that continues to challenge states in different areas of interactions. A prime example of this complexity is the "cybersecurity dilemma", where computer network intrusions undertaken for defensive purposes can be misinterpreted as preparation for an attack between states (Buchanan, 2017). This dilemma not only exacerbates the existing uncertainty regarding the intentions and capabilities of states in cyberspace but also contributes to an already competitive geopolitical environment in the Asia-Pacific. In this context, strategies developed in response to this uncertainty are influenced by states' interpretation of cyber threats and vulnerabilities, which invariably manifest in the type of policies states undertake (Lawson, 2013). Strategic culture therefore plays an important role in shaping the cyber strategy of small states because threat frames and policy discourses advanced by national security communities are anchored on the beliefs and practices derived from these states' historical experiences, limited resources, geographical constraints and national ideology.

The relevance of ideational factors in influencing the foreign and security policies of states in the Asia-Pacific Region has been well-documented in previous studies such as Ball (1993), Booth and Trood (1999), Kao (2011), Mahnken and Blumenthal (2014), Lantis et al. (2014), and Tellis, et al., (2016). This builds on these studies in two ways. First, it traces the contribution of strategic culture in shaping cybersecurity strategy of small states. Second, it explicates the role of strategic culture as a secondary condition in affecting the strategic preferences of small states coping with the relative distribution of power in the Asia-Pacific Region.

### *Contribution to cyber strategy*

The influence of strategic culture in shaping foreign and security policies has been established by previous studies but the contribution of cultural factors to the development of cybersecurity strategies remains relatively unexplored. It is tempting to presume that strategic culture shapes cyber strategies in the same manner as foreign and security policies because cybersecurity is treated as a foreign policy issue. However, recent studies present two crucial reasons why strategies for cyberspace are distinct. First, cyberspace is different from the traditional domains of military operations so the influence of strategic culture on this domain is still in the process of being defined (Wirtz, 2015). Second, the development of national strategies for cyberspace is still in progress however, current understanding about the role of strategic beliefs and practices in shaping these strategies is limited to the case of powerful states (Thomas, 2009; Adamksy, 2011; Giles, 2016). Following these reasons, this subsection compares the three cases by investigating the influence of their respective strategic cultures on their specific cybersecurity strategies.

The influence of strategic culture is difficult to assess but can be teased out from the content of the cyber strategies of the selected small states. How states interpret national security threats is central to how they develop and execute their respective strategies. In this sense, the strategies of both New Zealand and Singapore reflect a pragmatic interpretation of cyber threats, moving away from overstated or inflated assumptions that have influenced the policies of more powerful states (e.g. Lawson, 2013; Cavelty Dunn, 2015). Whereas the strategies of both states emphasise similar key objectives – resilience, capability building, cybercrime, and international cooperation – the proposed measures that each state has declared in their respective strategies reflect the influence of strategic culture.

In New Zealand's case, anti-militarism is manifested in the pacifist outlook of its cyber strategy. This assertion is based on the proposed measures that are unique to New Zealand such as Project Cortex and the "cyber credentials" scheme. Project Cortex is an advanced technical measure (Deep Packet Inspection)[15] intended to protect selected government and consenting private sector organisations from foreign-sourced, technically sophisticated cyber threats (NCPO, 2015). The Snowden Revelations about mass surveillance activities motivated the public to question the potentially intrusive nature of the measure, however, repeated assurances from former Prime Minister John Keys together with the declassification of GCSB documents has mitigated public criticism against Cortex (Pullar-Strecker, personal communication, June 13, 2016; Heather Ward, personal communication, June 15, 2016). The "cyber credentials" scheme is another concrete reflection of the imprint of New Zealand's anti-militarism because the business-oriented purpose of building cyber credentials. The objective of the scheme is to influence small and medium enterprises (SME) to comply with a specific set of cybersecurity standards. The scheme is driven by economic rather than national security interests because robust and secure digital environment contributes to productive and efficient businesses, which invariably helps the economic growth of New Zealand (NCPO, 2015).

The culture of insecurity is reflected in defensive thrust of Singapore's cyber strategy. This claim is supported by two proposed measures: decisive responses to cyber threats and collective responsibility for defence. In contrast to

[15] Deep Packet Inspection is a technology involving the intrusive observation of data moving through Internet Protocol (IP) networks (Corwin, 2011).

New Zealand's pacifist posture, Singapore's decisive and systemic response to computer network attacks is informed by its strategic beliefs and practices that condition a robust and pre-emptive response to national security threats. Consistent with this, the state has created a national cybersecurity response plan that enables "timely response and ground initiative at local level, complemented with effective coordination and strategic support at the sectoral and national level" (CSA, 2016, pp. 16-17).

Collective responsibility is an important component of the cyber strategy and is an important practice that is informed by Singapore's strategic culture. The logic behind collective responsibility is that all sectors of society are involved in securing the national interests of the state in the digital environment. In this environment, cyber incidents are treated as national security concerns, necessitating a comprehensive response from government as the lead coordinator but with contributions from other sectors such as private cybersecurity firms and international institutions. Collective responsibility is a strong indication of Singapore's culture of insecurity because it is an effort to compensate for the constraints confronting a small state, particularly the lack of human resource as well as strategic depth. In fact, this practice is one of the core ideas behind Singapore's main defensive framework of "Total Defence" or the "all-round response to threats and challenges and involves all Singaporeans" (Singapore Ministry of Defence, 2013). This practice is a sharp departure from New Zealand's strategic preferences as other sectors of society will oppose any effort by the government to further securitise cyberspace. Whereas New Zealand is working to mobilise various sectors to counter cyber threats, the measures involved in pursuing this effort is very different from Singapore because of the clear difference in strategic culture.

Brunei's strategy to manage cyber threats is summarised in several government documents, most prominently in the *Digital Government Strategy 2015-2020 (2015)* and *National Digital Strategy 2016-2020 ICT White Paper (2016).* However, the state does not have a standalone cybersecurity strategy unlike New Zealand and Singapore. The state recognises the significance of cybersecurity, however, the development of strategies and policies are predominantly dependent on the Sultan's approval since he is both the Head of State and the Prime Minister (Talib, 2002, 2013). The absence of a clear cyber strategy is indicative of

Brunei's measured progress towards building a network society. This predicament can be attributed Sultan's hesitation to harness the full advantages of technology and protect the state's prevailing strategic culture that is drawn from the MIB. Technological evolution is considered a risk to the Sultanate because of its potential to enable political revolutions through the diffusion of ideas and practices that empower population to challenge the status quo within states.

*Filtering strategic preferences*

The importance of strategic culture shaping the preferences of small states suggests that strategic belief and practices function as a filtering mechanism that can facilitate or impede the development of cyber capabilities within an environment conditioned by the relative distribution of power. It is this function that makes strategic culture a necessary secondary condition for the development of cyber capabilities. Networked technology exists regardless of a state's cultural preferences but structural constraints, specifically the imbalanced distribution of military capabilities in the Asia-Pacific Region conditions states to adapt and use networked technology for strategic purposes. This logic is consistent with the work of Ripsman et al. (2016) and Dueck (2011) that emphasises the significance of the filtering function of cultural variables in explicating the foreign policy behaviour of states.

Strategic culture is a mechanism that filters the development of cyber capabilities in small states such as New Zealand and Singapore but is an inhibiting mechanism in the case of Brunei. New Zealand's strong anti-militarist belief facilitates the state's inclination towards networked technology. Networks and computers enable states to achieve their foreign policy interests therefore New Zealand's main purpose in developing cyber capabilities is limited to protecting its economic and security interests, consistent with its strategy for securing cyberspace through capacity building and norm promotion.

Singapore's insecurity is a crucial factor in facilitating the state's orientation towards maintaining the technological edge in the Region but it is also this belief that distinguishes the state from New Zealand's interest in technology. While both states acknowledge the need for cyber capabilities, the insecurity driven by Singapore's inherent limitations and perceived threats has conditioned its preference for more extensive, military-oriented computer network capabilities that can support its highly capable military force in the event of military conflicts in the Region. Indeed, this direction is consistent with Singapore's strategy of leveraging advanced technology to ensure that it can thrive in a competitive geopolitical environment.

Brunei's conditioned strategic culture impedes the state's disposition towards the investment in networked technology necessary for the development of cyber capabilities. While the same structural pressures experienced by New Zealand and Singapore condition Brunei, it has yet to leverage the full potential of networked technology primarily because these can potentially contribute to disruptive ideas that challenge the prevailing traditional beliefs and practices anchored on the state's national ideology. Brunei's case illustrates that despite the advantages afforded by networked technology, the beliefs and practices of a state are still dominant in influencing strategic preferences.

## Strategic culture and government agencies

The significance of cultural factors in influencing states to designate agencies responsible for coordinating national cybersecurity initiatives has not been explored in any previous studies. The most relevant works that touch on the issue examine the contribution of strategic culture in shaping the preferences of great powers such as China (Hwang, 2012), Russia (Adamsky, 2017), and the U.S. (Harris, 2014) in exploiting the strategic advantages of cyberspace for military purposes but without considering the overall cyber strategy of states that include other civilian government agencies. Government agencies tasked to implement cyber strategies are not only critical to the success of the strategy but also suggest the type of approach that state intends to pursue in securing cyberspace. This subsection aims to fill this gap by tracing the contribution of strategic culture as a filtering mechanism in assigning the government agencies responsible for cybersecurity in small states.

New Zealand's anti-militarism extends to the designation of government agencies responsible for carrying out its cyber strategy. There are two key agencies involved in the cyber strategy of New Zealand: the National Cyber Policy Office (NCPO) and the GCSB. The primary coordinator for cybersecurity efforts of New Zealand is the NCPO, a unit under the Department of Prime Minister and Cabinet (DPMC) that is composed of diplomats and policy analysts specialising on technology (Heather Ward, personal communication, June 15, 2016).

The NCPO is responsible not only for developing the state's overall cyber strategy but is also in charge of coordinating the implementation of the *National Plan for Cybercrime 2015*, a supplementary strategy that is aligned with New Zealand's cyber strategy. This prescribes an interagency approach in addressing cybercrime therefore, even if the New Zealand Police has the "overarching responsibility for crime prevention" detection and investigation", it is apparent that the implementation of a national plan is not centralised with law enforcement authorities (NCPO, 2015).

The GCSB on the other hand is the principal government agency assigned to implement the state's cyber strategy in coordination with the NCPO. A key mandate of the GCSB is signals intelligence collection but it also the lead implementing agency for countering cyber threats through the National Cyber Security Centre (NCSC) which "provides enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats" (GCSB, 2017). The mandate of the NCSC is important to note because it clarifies the compartmentalization between the GCSB as a collector of signals intelligence and the main agency for information security. In terms of organisation, the GCSB is similar to the NCPO and is composed of staff from "a wide range of disciplines including foreign language experts, communications and cryptography specialists, engineers, technicians and corporate staff" (GCSB, 2016).

While the military is typically the main actor in matters of national security, the contribution of the NZDF is limited in the area of cybersecurity. The reason for this arrangement is New Zealand's aversion towards the militarisation of cyberspace, a move that is unnecessary and contradicts the state's beliefs and practices regarding the use of ICTs. In fact, the primary purpose of the Ministry of Defence in investing in cyber capabilities is to protect the network information systems, platforms, and personnel of the NZDF from computer network attacks (New Zealand Ministry of Defence, 2016, p. 76). Despite the increasingly sophisticated case cyber intrusions in the Asia-Pacific Region, there is no evidence to suggest that New Zealand will designate its military as the lead government agency for cybersecurity.

There are two implications that can be derived from New Zealand's preference to designate these government agencies. First, the state's anti-militarist culture functioned as a filter that influenced the preference for establishing a coordinating agency that is composed of diplomats and policy specialists. While powerful states such as China, Russia, and the U.S. appoint law enforcement, intelligence or military officials to coordinate national cyber strategies, the choice of staff from the Ministry of Foreign Affairs and Trade signifies the state's moderate interpretation of cyber threats. Second, while the GCSB is accused of conducting mass surveillance on its own citizens because of its arrangement with the Five Eyes, its stated contribution to the state's cyber strategy focuses on information assurance and capacity building (cf. Patman and Southgate, 2016; Rogers, 2015; Walsh and Miller, 2016). This is a more passive and less intrusive role compared to what is portrayed in previous studies (cf. Hager, 1996; Weller, 2001; Brunatti, 2012; Rogers, 2015; Patman and Southgate, 2016). The role is not only filtered by New Zealand's strong culture of anti-militarism but also supports the state's mandate of prioritising national interests over any defence or intelligence agreement.

Singapore's culture of insecurity is also ingrained in its choice of government agencies responsible for implementing its cyber strategy. There are three main agencies involved in Singapore's cybersecurity efforts: the Cyber Security Agency (CSA), the Singapore Police Force (SPF), and the SAF. The CSA is the principal agency "to oversee and coordinate all aspects of cybersecurity" in Singapore. Similar to New Zealand's configuration, the CSA functions under the Prime Minister's Office but a notable difference between the two states is that a former career senior military general is appointed to manage the agency. This arrangement suggests a more pre-emptive approach to cybersecurity that is linked to its culture of insecurity. This insecurity is based on the defensive mentality that adversaries will challenge Singapore's technological superiority through computer network attacks given the state's overdependence on ICTs.

The SPF is also a key actor in Singapore's cyber strategy because of its mandate to counter incidents of cybercrime. In contrast to New Zealand, the implementation the state's *National Cybercrime Action Plan* is assigned to the Ministry of Home Affairs, particularly the SPF. Whereas New Zealand implements an interagency approach to manage cybercrimes, Singapore prefers a more centralised approach, establishing a Cybercrime Command to increase "the agility and effectiveness of the SPF to respond to cybercrimes" by integrating "cyber-related investigation, forensics, intelligence and crime prevention capabilities within a single command" (Singapore Ministry of Home Affairs, 2016, p. 11). The preference for centralisation is a reaction to the Singapore's insecurity that demands a more integrated and faster response to counteract cybercrimes. Cybercrimes are a source of insecurity because they may involve governments of hostile states and cybercrimes directly undermine one of Singapore's core national interests: robust economic growth.

Another considerable difference between New Zealand and Singapore in designating government agencies for cybersecurity is the more prominent role of the military in Singapore's strategy. The SAF is more involved in the state's cybersecurity efforts because of Singapore's culture of insecurity that demands a more proactive strategy in addressing cyber threats. Two indicators support this assertion. The first indicator of Singapore preference for military involvement is its cyber strategy is the establishment of a cyber command. Singapore is the first small state to officially publicise the establishment of a military cyber command in the region – the Defence Cyber Organisation (DCO). The DCO's main responsibilities are to develop cyber defence strategies and policies as well as to enhance capability development but it is also authorised to support the CSA in strengthening the state's overall cybersecurity. Disclosing the existence of a cyber command is a strategic move for Singapore because it signifies that the state is capable of defending its interest in cyberspace and is prepared to utilise the military to manage the insecurity regarding the capabilities and intentions of potential adversaries in cyberspace.

The second indicator of the military's prominent role is that the same chief executive, who was formerly a general with the SAF, manages both the CSA and DCO despite the clear distinctions between the orientation of both government agencies. The CSA is a civilian organisation mandated to coordinate with all sectors of society as well as other states and the DCO is a military organisation created to protect the networks and systems of the defence community. This predicament is important because it indicates Singapore's preference for the greater involvement of the military in enhancing its cybersecurity posture. The culture of insecurity has compelled the state to increase its dependency on the military even if cyberspace is not necessarily a warfighting domain (Libicki, 2012).

Singapore's preference for designating specific government agencies teases out two points for analysis. First, its strategic culture of insecurity has filtered Singapore's preference for greater military involvement in its approach to securing cyberspace. This is clearly reflected in the measures it has implemented and agencies created in line with its cyber strategy. Second, Singapore's insecurity has filtered its preference for considering technological innovation as both an advantage and a threat. The state's ambition to become a "Smart Nation" that is the leader in technological innovation in the Asia-Pacific Region is supported by a robust cyber strategy managed through a pragmatic and militaristic outlook.

The conditioned strategic beliefs and practices of Brunei filter the state's designation of agencies responsible for cybersecurity. There are two main government agencies involved in Brunei's cybersecurity efforts: the National Security Committee (NSC) and the Internal Security Division (ISD). Like New Zealand and Singapore, these agencies are coordinated through the Prime Minister's Office (PMO) but the clear difference with Brunei's governance structure is the high degree of centralisation in implementing its cyber strategy. This centralised structure is more similar to Singapore more than New Zealand because the CSA, which is supervised the Prime Minister's Office, plays a greater role in the operational aspects of state's cyber strategy. New Zealand's approach is less centralised since the NCPO mainly focuses on coordinating the policy and the execution of the actual strategy is left to the different agencies. Brunei's highly centralised governance structure is indicative of the conditioned strategic culture of Brunei because it affirms the power and authority of the Sultan in governing all aspects of the state especially ICTs, which is viewed by the government as a tool to instigate of political discord and mobilise uprisings against the Sultanate (Criossant and Lorenz, 2018, pp. 27-29).

Brunei's NSC is the main government organisation that coordinates all efforts pertaining to national security and is composed of the career government officials all appointed by the Sultan. Through its Cyber Security Working Committee, the NSC advises the Prime Minister about emerging cyber threats, proposes policies, and directs national cybersecurity efforts (Brunei Prime Minister's Office [BPMO], 2016). The ISD on the other hand, is the intelligence and security agency of Brunei. In terms of cybersecurity, the ISD is responsible for monitoring incidents relating to subversion, espionage and sabotage through computer networks as well as the implementation of the information security policies in Brunei (BPMO, n.d.). The Permanent Secretary for Security and Enforcement coordinates the secretariat of NSC and manages the operations of ISD, reinforcing state's tightly controlled governance structure.[16]

The preference of a tightly controlled security environment that is focused on internal security threats is consistent with the state's conditioned beliefs and practices that influences the management of its intelligence agencies as well. The literature on intelligence culture offers some insights that can supplement strategic culture. Studies in this area contend that non-democratic states use intelligence agencies to ensure regime survival. More specifically, these states "use their intelligence apparatuses (known as "political polices") to control, intimidate, manipulate, abuse, and oppress real and/or imaginary "ideological enemies," both domestically and abroad…" (Bruneau and Matei, 2010, p. 729). This is consistent with Brunei's experience considering that its law enforcement and intelligence agencies are mandate to arrest any person suspected to be a national security threat without evidence or a warrant (Croissant and Lorenz, 2018, p. 28). In this sense, the state's conditioned beliefs and practices combined with the leadership's motivation for regime survival can provide additional insights regarding Brunei's foreign policy behavior.

One key insight is the state's comprehensive approach to maintain its survival. The Sultanate consolidates its legitimacy and influence through its national ideology. This is reflected in its strong influence in shaping the state's strategic preferences. However, these beliefs and practices are reinforced through a stringent national security system. Indeed, Brunei is more concerned with internal rather than external security threats, and this is clearly reflected in the configuration of its military forces, the mandate of its security and intelligence agencies, and the rationale for stationing British military forces within the state (Cheng-Chwee and Welsh, 2008, pp. 63-65).

Another important insight is the state's reluctance towards building a highly networked society. This behaviour is manifested in the strong government content control on ideas that challenge the beliefs and practices articulated by the national ideology. Limiting the flow of information is instrumental in preserving

[16] (Retired) Lieutenant Colonel Pengiran Haji Muhamad Sazali bin Pengiran Haji Yakob was appointed as Permanent Secretary for Security and Enforcement in January 2018.

the status quo: "The meaning people draw from information depends on pre-existing ideas and values that can change slowly even when new information calls those views into question." (Lord, 2006, p. 183). In this context, the Sultanate's survival depends on how effective they manage the consequences of their political policies: lack of public awareness, media coverage and policy debates regarding cybersecurity issues.

## Conclusion

This chapter explicated how a strategic culture is a necessary secondary condition that refines the responses of small states to the relative distribution of power in the region. This was achieved through the development the concept of technology-oriented strategic culture and through investigating three observable implications: network readiness, cybersecurity strategy and government agencies responsible for cybersecurity. The concept of technology-oriented strategic culture was introduced in the chapter to clarify the interplay between culture and technology in the relation to the foreign policy preferences of small states. A technology-oriented strategic culture can be characterised by five attributes: information-driven, draws on pervasive technologies, applies network logic, uses technology for external affairs and social engagement. These attributes are useful in describing the concept of technology-oriented that describes the tendency of small states to depend on technology to compensate for their strategic limitations in materials capabilities.

The connection between strategic culture and network readiness was established by exploring the sources of strategic culture and how these shaped the strategic preferences of small states. The chapter argued that geography and natural resources were key sources of strategic culture that motivated the high level of network readiness of New Zealand and Singapore. However, despite being affected by similar constraints, Brunei's move towards developing a highly networked society has lagged behind because of cultural factors particularly the limitations prescribed by its national ideology, Malay Islamic Monarchy. This national ideology therefore is the differentiating factor that refines the impact of external constraints on the preference of Brunei to develop cyber capabilities.

The contribution of strategic culture as a secondary condition that that directs cyber strategies of the three states was examined through a survey the prevailing strategic culture and an analysis of how these beliefs and practices filter responses of small states to cyber conflicts in the region. The chapter demonstrated that strategic culture of both New Zealand and Singapore influenced their respective approaches to cybersecurity in the context of a regional environment conditioned by the relative distribution of power. This suggests that while strategic culture is a necessary condition that directs the preferences of small states, it is only secondary to the relative distribution of power that is the principal condition that shapes the environment that necessitates the development of cyber capabilities. New Zealand's anti-militarist culture shaped the pacifist outlook of its cyber strategy as manifested in the diplomacy-centred approach the state has adopted to counter cyber threats. Singapore's deep-seated culture of insecurity was persuasive in developing pre-emptive cyber strategy reflected in the military-centred approach of the state towards securing its interests in cyberspace. In the case of Brunei, strategic culture impedes the efforts of the state towards building a digital environment necessary for the development of cyber capabilities. Whereas the same geopolitical constrains affect Brunei, it has not taken advantage of the full potential of networked technology mainly because of the disruptive potential of the Internet that can challenge the dominant beliefs and practices anchored on the state's national ideology.

The influence of strategic culture on the designation of government agencies responsible for cybersecurity was traced through an assessment of the governance structure in coordinating cybersecurity efforts. The chapter confirmed that strategic culture reinforced the selection of specific government agencies in supporting the states' approach to cybersecurity. New Zealand's predisposition for a more diplomatic and passive approach in securing cyberspace is consistent with its anti-militarist strategic culture. Following this approach, New Zealand's structure for coordinating cybersecurity is focused on an interagency effort with diplomats and policy specialists leading the effort.

Singapore's preference for militaristic approach to cybersecurity is conditioned by its previous experiences with its neighbours. This outlook has influenced the state to assign military officials to coordinate national cybersecurity efforts as well as to expand the role of its military forces in defending the network and systems across the state. Brunei's centralised and tightly managed governance structure for cybersecurity is in line with its strategic beliefs and practices that are conditioned by its national ideology. It is the priority of Sultanate to maintain the social and political status quo in Brunei therefore managing the diffusion of ideas that can challenge the national ideology and mobilise subversive action is vital to the survival of the state. In this sense, the Prime Minister's Office controls all initiatives and actions relating to networked technology and the dissemination of information.

Having addressed the main puzzle of the study, the next chapter evaluates the strategic utility of cyber capabilities as an instrument of foreign policy. Previous studies on the topic have mainly focused on the value of cyber capabilities as enablers of conventional military capabilities, however, the functionality of cyber operations for other aspects of foreign policy such as diplomacy and covert action remains uncharted. Chapter 6 assesses the utility of cyber capabilities for small states by evaluating the conditions under which cyber capabilities can be advantageous for small states and by integrating cyber operations within the foreign policy arsenal of states.

# Chapter 6
## Cyber Capabilities as a Foreign Policy Instrument

The revolutionary impact of information and communication technologies on military and strategic affairs continues to be an unresolved subject of debate for scholars and policymakers who seek to understand the contribution of cyber capabilities in the foreign and security strategies of states. The idea that technology can empower weaker states to compete with or challenge the strong is so persuasive that it has influenced states to employ exaggerated responses to cyber threats that are often misunderstood (Rid, 2013; Lawson, 2013; Dunn Cavelty, 2015). Great powers have been decisive in testing cyber operations for espionage and sabotage because these states have the resources, expertise, and the intention to harness the advantages of ICTs. However, the use of ICTs remains unclear for less powerful states that are still trying to cope with the complexities of cyber interactions. Indeed, small states such as New Zealand and Singapore are confronted with a difficult dilemma: they have developed cyber capabilities without a well-defined understanding of the utility of these instruments.

The preceding chapters addressed the main and the first corollary research questions by explicating the necessary conditions for small states to develop cyber capabilities. Chapter 4 argued that the relative distribution power in the Asia-Pacific Region is the primary condition that affects the development of cyber capabilities. The imbalanced distribution of power or material resources between great powers and other states has generated uncertainty and mistrust that has manifested in the cyber domain through the prevalence of cyber conflict in the region (Valeriano and Maness, 2015). Small states are therefore compelled to adapt to this predicament by developing their own cyber capabilities to protect their respective foreign policy interests. This structural condition however, is insufficient to understand why small states developed cyber capabilities because of the domestic constraints confronting these states. In this sense, Chapter 5 explored strategic culture as a secondary condition that filters the strategic preferences of small states. Strategic culture affects the development of cyber capabilities because strategic beliefs and practices of small states influence their interpretation of cyber threats as well as the strategies that govern the use of cyber capabilities.

After establishing the conditions necessary for cyber capability development, this chapter focuses on answering the second corollary question presented in Chapter 1: the advantages and limitations of cyber capabilities. More precisely, the chapter addresses the dilemma confronted by small states by clarifying the utility of cyber capabilities as a foreign policy instrument for small states. States have used ICTs to shape the behaviour of other states hence cyber capabilities can be considered as foreign policy instruments or "specific options available to policy makers for exerting influence on to other actors in the international system" (Smith, et al. 2016, p. 299). In pursuing this objective, this chapter focuses on evaluating the applicability of existing strategic concepts to the cyber operations and assessing the usefulness of cyber capabilities for New Zealand, Singapore, and Brunei. The following questions are addressed to facilitate concept building and the comparison of cases in the chapter:

1. What makes cyber capabilities useful for small states?
2. How are cyber capabilities integrated within the foreign policy continuum?
3. Which networked-enabled instruments of foreign policy are feasible tools for small states?

The remaining parts of this chapter are divided into three sections. The first section evaluates the conditions under which cyber capabilities can be advantageous for small states. The second section situates cyber capabilities within the foreign policy arsenal of states, while assessing the feasibility of cyber operations for the three cases selected for the study. This analysis is vital because existing studies mostly consider cyber capabilities as an enabler of military force and not as a broader instrument to advance foreign policy (cf. Libicki, 2007; Rid, 2013; Gray, 2013). The last section summarises the key arguments of the chapter and links the ideas discussed with the rest of the thesis.

## Small states and the use of cyber capabilities

Advancements in technology have influenced the diffusion of power in the twenty-first century. Cyberspace, a product of this technological evolution, facilitates the rapid exchange of information, allowing states to interact and compete for strategic resources necessary to thrive in a complex international system. However, even with the pervasive impact of technology, the distribution of power has not balanced out and great powers are still in the stronger position to use cyber capabilities in advancing their respective interests (Lindsay, 2013; Valeriano et al., 2018).

The power imbalance in cyberspace has several implications for small states that are technologically oriented but are constrained from using cyber capabilities due to both material limitations and cultural preferences. The distinctive characteristics of cyber power make computer network operations advantageous particularly when they are employed to supplement existing foreign policy instruments. Despite this potential advantage, the utility of cyber capabilities needs to be clarified when it comes to small states such as New Zealand, Singapore, and Brunei. As discussed in preceding chapters, these states developed cyber capabilities because they were compelled to adapt to the prevailing structural conditions and not really because of the perceived revolutionary impact of network technologies. To address these implications, this section draws from the characteristics of cyber power presented in Chapter 1 and presents two fundamental conditions that enable small states to effectively employ cyber capabilities as an instrument of foreign policy.

The first basic condition is that small states need to have a capable technology-oriented military force to derive advantages from using cyber operations. Since cyber capabilities are predominantly used to supplement or amplify existing military capabilities in advancing foreign policy, it would be counterintuitive for small states with limited military capabilities to invest in cyber capabilities because these cyber operations cannot produce decisive strategic outcomes (Gray, 2013). Moreover, small states that have limited engagement with network technologies for managing national security issues will have less interest in using cyber capabilities as a foreign policy tool. The premise that cyber capabilities are valuable tools for asymmetric warfare is therefore problematic when applied to New Zealand, Singapore, and Brunei because not all of these states have the military capacity as well as the intention to use cyber operations proactively against other states. Following this logic, small states would maximise the use of cyber capabilities if these operations were conducted in support of different foreign policy functions such as diplomacy and political intervention in addition to warfighting. The stealthy and functional characteristics of cyber power support this assertion.

Cyber operations are stealthy because detecting cyber intrusions is more complicated than conventional military attacks. Indeed, it takes a combination of different factors such as skills, time, management, leadership, and recognition of the limitations of attribution (Rid and Buchanan, 2014, p. 4). These intricacies make cyber capabilities useful for small states because they can be utilised for other operations aside from warfighting such espionage, sabotage, subversion and hacktivism or online political protests. These measures have been employed by states long before computers were created, however using computer networks to carry out these interventions increases the complexity of these operations because of the predisposition of cyberspace for deception and manipulation (Lindsay and Gartzke, 2015). Cyber capabilities are therefore useful as tools for foreign policy because in the event of heightened tension, small states can use cyber operations for covert communication: to demonstrate the capacity to operate in cyberspace and to signal resolve in countering the risk of military escalation with adversaries (Carson and Yarhi-Milho, 2017, pp. 133-135). However, this function is only effective if the covert message is visible to a specific target audience such as a strategic adversary. The literature on covert signalling suggest that the robust information collected and assessed by intelligence agencies provides rivals the ability to understand "the basic contours of covert behavior" (Carson and Yarhi-Milho, 2017, p. 132) or "an ad hoc set of ground rules" (George cited in Carson and Yarhi-Milo, 2017, p. 132) which in turn enables them to interpret covert messages by rival states. In this context, the strategic use of cyber capabilities requires small states to consider the appropriate conditions and specific target audience before employing them to advance their foreign policy interests.

Disrupting the normal functions of a state anonymously can mitigate military conflict because there is no logic in mobilising military forces if there are no clear targets. A parallel example that supports this argument are the insistent DDoS attacks against South Korean government agencies and private sector websites by groups indirectly linked to North Korea (cf. Wicherski, et al., 2011; LaMontagne, et al., 2016; Kamluk, et al., 2017). These incidents were documented as far back as 2009 and continue to persist today (Jun, et al., 2015; Segal and Grigsby, 2017). The objective of these intrusions is to constantly undermine South Korea's national interests by temporarily disrupting the essential functions of the state governance such as basic utilities and financial institutions. Despite these persistent intrusions, the cyber conflict between the two states has not escalated to military conflict or deployments therefore demonstrating the potential of using cyber capabilities to avoid violence or physical harm.

On the other hand, willingly claiming credit for cyber intrusions can also be useful for small states because it allows states to convey discontent about foreign policy issues without escalating to conventional military conflict. Indeed, while operational secrecy is a necessary requirement of all cyber operations, "concealing one's sponsorship afterwards is a strategic calculation" (Poznansky and Perkosky, 2018). The Hainan Island Incident in 2001 is a relevant example that supports this argument because it involved cyber actions that were acknowledged by patriotic hackers passively supported by China. The incident was provoked by a mid-air collision between a Chinese J-8 fighter and a U.S. P-3 surveillance aircraft that caused the death of a Chinese pilot and forced the U.S. military aircraft to land in Hainan Island.

This collision inspired multiple website defacements by Chinese patriotic hackers against a range of targets including U.S. public libraries and government institutions such as the White House (Singer and Friedman, 2014, pp. 113-114). While these patriotic hackers or "cyber proxies" were not officially ordered to attack the U.S., their actions can theoretically be attributed to China depending on the state's relationship with a proxy during the time of the incident (Maurer, 2018, p. 129).[17] A recent study on the role of non-state actors in cyber conflict suggests that China maintained a "sanctioning" relationship with cyber proxies where "the state provides an enabling environments for non-state actors' malicious activity be deliberately tuning a blind eye to their activities" (Maurer, 2018, p. 21). In this context, the U.S. could have challenged China to crackdown and penalise on patriotic hackers but the mechanisms for accountability both legal and political were still incipient during the time of the incident.

The functionality of cyber operations is limited for small states because these states are unlikely to exploit the offensive advantages of cyber operations and transitory or temporary ability of cyber weapons to inflict harm or damage. The most sophisticated cyber capabilities are developed by powerful states

[17] "A *cyber* proxy is therefore an intermediary that conducts or directly contributes to an offensive *cyber* operation that is enabled knowingly, actively or passively, by a beneficiary who gains advantage from its effect (Maurer, 2018, p. 31).

because these actors have access to considerable resources, expertise, and intelligence regarding other states. Small states are not capable of competing with the "cyber powers", therefore, using offensive cyber operations has limited value for the less powerful. While non-state actors such as terrorist organisations or transnational organised crime groups are also confronted by the same barriers, the key difference is that small states are more vulnerable to cyber incidents since they are fixed targets that are dependent on CNI necessary for protecting a basic public services for maintaining a minimum level of law enforcement, public safety, economic activity, and public health (Dunn, 2006, p. 34). In contrast, non-state actors are more flexible and are less vulnerable to cyber operations given that these actors do not maintain any specific territory and are not responsible for defending any CNIs for survival. Small states are also in a weak position to capitalise on the transitory nature of cyber weapons because these states do not have the monopoly of advanced ICTs. Even if small states have access to unique and complex technology, it would be difficult for them to weaponise and execute cyber operations that "cause significant physical damage" (Lindsay, 2013, p. 402).

In the case of small states, the functionality of cyber operations more focused on network defence. Although defending computer networks is not a function that actively supports foreign policy, defending computer networks are essential to the national security of states in the twenty-first century. Indeed, highly networked small states are more vulnerable to cyber incidents because they rely significantly on ICTs but cannot credibly deter adversaries from executing attacks both in the conventional and digital domains (Lindsay and Maness, 2018). An example of defensive cyber strategy utilised by a small state is Georgia's move to protect its critical digital assets from Russian cyber operations in the context of the Russia-Georgia Conflict in 2008.

Georgia's ability to manage essential public services was severely disrupted by multiple and concentrated DDoS attacks against vital websites that placed the state in a precarious and helpless situation. Since the state did not have sufficient resources to directly counter or retaliate against comprehensive DDoS attacks, it was forced to come up with a creative survival strategy by transferring its critical digital assets to servers located Estonia, U.S., and Poland (Gamreklidze, 2011, p. 211). The objective of the move was to demonstrate resolve against Russia and ensure the continuity of crucial government operations such as media releases by the government ministries and statements from the President of Georgia (Korns and Kastenberg, 2009, p. 60). While a single case can only produce limited generalisations, it is reasonable to argue that the functionality of cyber capabilities is reduced for small states because the full range of functions facilitated by the unique characteristics of cyber power are not necessarily realistic for these states. The literature suggests two examples to support this assertion.

The first is covert action measures such as *Operation Olympic Games* that cause kinetic or physical damage. It is unlikely for small states to engage in cyber operations that cause physical damage against a more powerful state because of the potential retaliatory measures that can involve more complex cyber intrusions. It would also be impractical for small states to utilise the same measures against other less powerful states because the substantial resources involved in executing cyber operations that cause physical damage (Slayton, 2017). The second is cyber operations to support military action. It is disadvantageous for small states to utilise cyber capabilities to support coercive operations and warfighting if they do not have capable and credible military force that is acknowledged by other states in the region. Cyber capabilities are ineffective stand-alone instruments of foreign policy because cannot directly produce strategic outcomes. A more details discussion of these points is presented in the next section of the chapter.

The second basic condition for cyber capabilities to be useful for small states is that these are employed to pursue a limited objective: signalling foreign policy preferences. This can be achieved through low-level cyber skirmishes to reduce the possibility for any escalation to kinetic conflict. The specific functions useful to small states will be discussed in the next subsection but the logic behind cyber intrusions is to send a strong political message without directly provoking military action. Depending on the objective, small states can convey messages through cyber operations in two ways. One is through private acknowledgement in a situation where an attacker discreetly alerts the target state of its culpability. This can be done by leaving clues during a course of an intrusion such as digitally signing a "code under a certificate that is publicly known to be associated with" a specific government (Goldsmith, 2012). Another method is through public acknowledgement, in a scenario where the attacker openly discloses their identity thereby confirming sponsorship. Public acknowledgement eliminates the attribution problem and can be done when the attacker alerts the media of their responsibility for the incident (Poznansky and Perkoskizy, 2018).

The function of signalling is supported by the unique characteristics of cyber power, specifically the nonphysical and pervasive features of cyber operations. The non-physicality of cyber capabilities make them practical instruments for small states because cyber intrusions are considered less threatening than other intrusive foreign policy tools. Since cyber operations do not cause direct physical harm or violence, international institutions such as the United Nations consider a conventional military response to cyber incidents as disproportionate (O'Connell, 2012, pp. 198-202). Moreover, since the damage inflicted by cyber operations on physical objects is not permanent states are therefore incentivised to restrain their responses to computer network attacks.

Based on these two conditions, the perceived strategic utility of cyber capabilities is not as revolutionary as some scholars and policymakers claim. Whereas the pervasive nature of cyber power enables small states to develop alternative methods of conveying foreign policy interests to adversaries, this function remains as the most feasible for the use of cyber capabilities by less powerful states. Indeed, failing to respond appropriately to cyber incidents can be consequential because it can involve "audience costs" or penalties imposed by domestic and foreign audiences on leaders (Fearon, 1997, p. 70). These costs arise from the reaction of domestic and international audiences "interested in whether foreign policy is being successfully or unsuccessfully handled by the leadership" (Fearon, 1997, p. 69).

A relevant example of audience cost in relation to cybersecurity is the fallout in New Zealand due to the global surveillance disclosures of Edward Snowden. The disclosures generated problems because of the report that New Zealand's signals intelligence agency, the GCSB, was violating its primary mission of "protecting and enhancing New Zealand's security and wellbeing" (GCSB, 2016, p. 8). Since the GCSB is a contributor to the Five Eyes intelligence network, it monitors leaders and activities of various states including allies in the Pacific Islands even if these people and states are not treats to New Zealand. While the government was able to manage the short-term political and diplomatic fallout, the continued lack of transparency regarding the participation of the GCSB in the Five Eyes can still create a credibility gap that can certainly damage the political legitimacy and diplomatic image of New Zealand in the long-term

(Patman and Southgate, 2015; Young, 2015). In this context, the failure to clarify the extend to the GCSB's computer network exploitation contributed to audience cost particularly the weakened public trust in the GCSB (Stewart, 2015) and the damage reputation of New Zealand a reputable global trading partner (Edwards, 2015).

## Cyber capabilities and foreign policy

The use of cyber capabilities to advance political objectives is the "new normal" in the foreign policy interactions between states (Valeriano*,* et al.*,* 2017). States typically infiltrate and disrupt networks of adversaries to with the objective of signalling foreign policy preferences and collecting intelligence. States can utilise cyber capabilities strategically by conducting publicly acknowledged intrusions to convey revolve and capability or privately acknowledged intrusions to coerce an adversary to comply with the preferences of the attacker (Poznansky and Perkosky, 2018). Cyber capabilities have been employed by states for different purposes as discussed in previous chapters however, systematic assessment that discusses the potential of these capabilities in supplementing existing foreign policy instruments has yet to be achieved.

The utility of cyber capabilities as a stand-alone strategic instrument of states continues to be a subject of considerable debates that remain unresolved (cf. Gartzke, 2013 and Kello, 2013). One view suggests that cyber capabilities are *independent* tools for covert action against adversaries (Kello, 2013, 2016; Brantly, 2014, 2016). A more dominant perspective contends that cyber capabilities are *adjunct* tools that strengthen other foreign policy instruments such as hacktivism, disruption, espionage, and military action (Rid, 2013; Lindsay et al., 2015; Borghard and Lonergan, 2017; Lindsay and Gartzke, 2018).

Since resolving this debate is not the objective, this study contributes to the literature by examining the contribution of cyber capabilities in supplementing existing foreign policy instruments. While a balanced perspective is necessary to develop a clear conceptualisation of cyber capabilities as a foreign policy instrument, existing studies on the subject have not presented any definitive arguments or strong empirical evidence that confirm the utility of cyber capabilities as a stand-alone instrument to advance foreign policy interests. For instance, Kello (2017, p. 4) argues cyber weapons are revolutionary strategic instruments because their impact on international order is "deeper and broader" than nuclear weapons. His works suggests that cyber weapons can be more disruptive power than nuclear weapons because their impact is subtler but more pervasive: "expansion of nonphysical threats to national security, the growing ability of nonstate actors to instigate diplomatic and military crises, the deep penetration of computer systems by undetected agents" (Kello, 2017, p. 4). Another study by Brantly (2016, p. 97) contends that states can utilise cyber capabilities as an independent tool to achieve specific strategic objectives. The logic behind this view is that the efficacy of cyber operations is predicated on whether the attacking targets that are enabled by or dependent on digital technologies. He makes the case for an independent function by classifying cyber operations as part of a "new typology of covert action" that states can exploit to achieve certain foreign policy objectives (Brantly, 2016, p. 43).

Whilst both scholars provide alternative interpretations of the utility of cyber capabilities, these works suffer from two weaknesses. First, the idea that cyber operations are new types of foreign policy tools is misleading. The perceived novelty of cyber capabilities is based on the special functions they can perform: the ability to inflict economic and political damage without resorting to violence (Kello, 2013) and the ability to "alter a bargaining range between two states prior to engaging in or in attempting to avert an overt war" (Brantly, 2014, p. 466). While the use of computer networks to execute these functions is relatively new, the outcomes and objectives of these operations are not. Negative sanctions (see Table 5) can inflict economic and political damage without necessarily resorting to violence and covert action involves different measures such as sabotage or subversion that can alter the bargaining range between states aside from cyber operations. Second, these scholars present questionable case studies to support their claims. *Operation Olympic Games* and *Operation Orchard* were cited as prominent cases to illustrate the stand-alone function of cyber capabilities (Brantly, 2016, pp. 58-60; Kello 2017; pp. 60-68). The problem however is that the cyber operations in these cases were not really utilised as stand-alone instruments because they were employed to reinforce or supplement other longstanding foreign policy strategies such as negative sanctions against Iran and potential military action against Syria in the case of *Operation Orchard* (Farwell and Rohozinski, 2012; Rid, 2013, pp. 42-46). Based on this assessment, this section focuses on the adjunct or combined function of cyber capabilities. The adjunct function is based on the idea that cyber capabilities "amplify the power of actors that have enough resources and expertise to figure out how to manage the complexity and uncertainty associated with ambitious intrusions" (Lindsay and Gartzke, 2018).

In this context, cyber capabilities are more useful as adjunct functions because they supplement rather than substitute other tools in the foreign policy arsenal of states. There are a number of cyber operations that can be categorised as adjuncts but at the level of foreign policy, these actions fall under *diplomacy, covert action,* and *military action.* Cyber espionage or intelligence collection through computer networks is discussed extensively in the literature but is not treated as a separate foreign policy instrument in this study for two reasons. First, espionage and covert action are interdependent activities: espionage is a prerequisite for covert action and covert operations are the implementation of intelligence collected from espionage. Second, the objective of espionage is to seek and safeguard information and not to directly influence the foreign policies of other states (Shulsky and Schmitt, 2002, pp. 8-9) therefore it is not strictly a foreign policy instrument. A similar argument can be for positive and negative sanctions. Employinh network technologies to supplement these functions do not produce anything instrumental (e.g. "networked-enabled sanctions") that can actively advance foreign policy. A more detailed discussion is presented in the second part of this section. This section proceeds in two parts. The first examines the role of cyber capabilities in amplifying foreign policy functions and argues that these capabilities have limited utility as foreign policy instruments for New Zealand, Singapore, and Brunei. In essence, these capabilities are not revolutionary foreign policy tools that enable the small states to change the dynamics of interstate conflict. The second part locates cyber capabilities as an instrument within the spectrum of foreign policy options available to states and contends that cyber capabilities are best considered as modified versions of existing instruments.

### *Diplomacy*

The first adjunct function is the use of cyber capabilities to enhance diplomacy. Digital diplomacy or the "strategy of managing change through digital tools and virtual collaborations" is the evolution of traditional diplomacy that is considered an essential foreign policy instrument of states in the twenty-first century

(Holmes, 2015, p. 15). ICTs are useful in enhancing the level of collaboration and interactions between states in three ways: it multiplies and amplifies the "the number of voices and interests involved in international policy-making"; it allows the rapid dissemination of information between states, and it facilitates of faster and more cost-effective delivery of traditional diplomatic services to citizens and other governments (Westcott, 2008, p. 2). In this sense, digital diplomacy is an adjunct function of cyber capabilities because it enables states to advance their diplomatic interests by utilising various digital platforms such as social media, mobile devices, and the Internet to shape narratives and debates on specific foreign policy issues. The UK's "diplomatic excellence" is a prominent example discussed in previous studies (Hague cited in Pammet, 2016, p. 1).

The UK's strategy towards institutionalising ICTs as standard tools for diplomacy is an archetypal case of the integration of ICTs in foreign policy engagement. The UK Foreign & Commonwealth Office (FCO) is a leader in the area of digital diplomacy (Clarke, 2015) because of its enduring commitment to harness the advantages of digital innovation by embedding "the use of digital across every element of foreign policy work" and provide all its "services digitally by default" (Foreign & Commonwealth Office [FCO], 2012, p. 2). The UK's strong commitment to use digital tools has been tested during crisis situations such as the Costa Concordia cruise ship incident in 2012 where the FCO exploited various digital platforms including Facebook and Twitter for strategic communication, to constantly update the public about the situation and document the response of the FCO's consular team on the ground in Italy (FCO, 2012, pp. 12-13).

Another example of the UK's digital diplomacy initiatives is the FCO's participation in the intergovernmental effort to combat terrorist propaganda. False ideas or propaganda can influence perceptions of disaffected people and since ICTs can amplify these ideas, disputing these messages is vital to national security. The FCO's specific contribution therefore is counter messaging or exposing the group's "delusional and false religious narrative" and disclosing facts and figures regarding the group's failures (FCO, 2014). Consequently, in addition to strategic communication, digital diplomacy contributes to counter propaganda, a fundamental element in the UK's national security strategy.

*Networked-enabled diplomacy and small states*

Diplomacy is an essential tool for small states because it affords the opportunity to project soft power by shaping the foreign policy preferences of other states by attracting other states through culture, values and policies rather than force of sanctions (Nye, 2004, pp. 5-8). Since using ICTs to shape state preferences is an established practice among states in the twenty-first century, digital diplomacy is a key instrument that small states can employ to thrive in a competitive geopolitical environment in the Asia-Pacific. Digital diplomacy has been an effective instrument for New Zealand and Singapore since the two states have engaged in "virtual enlargement" or measures such as good governance and diplomatic mediation (Chong, 2010) that expands their importance to the international community while Brunei remains careful with its engagement in the full spectrum of cybersecurity issues. These measures are manifested in three areas of diplomacy: norm promotion, international cooperation, and economic growth.

The advancement of norms or rules for state behaviour in cyberspace is a core diplomatic agenda for New Zealand and Singapore because they believe that this measure is a concrete step towards strengthening the cybersecurity of states in the region. Both states highlight the importance of developing the capacity for defence, establishing norms for cyberspace, and building confidence between states in countering cyber threats and reducing cyber conflicts in the region. A reputation for robust cyber capabilities is crucial to this diplomatic initiative because it signifies that New Zealand and Singapore have the capacity and credibility to implement what they are advocating for. Brunei, on the other hand, participates in advancing certain cyber norms particularly when it involves cyber crime but is not as aggressive as New Zealand and Singapore despite its increasing dependence on ICTs for its oil and gas production. As discussed in the previous chapter, Brunei's limited participation can be attributed to its conditioned strategic culture, which has been influential in shaping its foreign policy direction.

Strengthening international cooperation is another essential diplomatic agenda for New Zealand and Singapore. These states contend that since computer network attacks are not constrained by geographical boundaries and state sovereignty, cooperation is necessary at all levels of interaction in cyberspace. For instance, New Zealand is a leading advocate for a multi-stakeholder approach to Internet governance globally while Singapore has taken the lead in convening regular multi-track diplomatic dialogues on cybersecurity issues between principal stakeholders in the Asia-Pacific. In this sense, establishing a formidable reputation for cyber operations by disclosing certainly capabilities or public acknowledging responsibility for intrusions is instrumental considering the uncertainty regarding the behaviour of states in cyberspace. This effort contributes to New Zealand and Singapore's ability to advance their foreign policy interests because it strengthens national prestige and projects credibility, two characteristics that are instrumental in executing successful coercion strategies (Poznansky and Perkosky, 2018). Brunei's foreign policy interests are not in the same direction as the two states because it has yet to assume a leading role in advancing cybersecurity initiatives, nor has it actively participated in sponsoring cyber issues in regional and international institutions.

Enhancing economic growth is the third core interest that is listed in the cyber strategy of New Zealand and Singapore.  The strategy for these two states has been to leverage on their existing cyber capabilities to establish and promote a secure and trusted digital environment that is attractive to multinational and technology companies, thereby increasing the potential for more foreign investments. This agenda is systematically reinforced through the idea of creating a "digital nation" in New Zealand (Muller, et al., 2016) and the implementation of the Smart Nation Platform in Singapore (IDA, 2014), both of which are discussed in Chapter 5. While these initiatives have different objectives, they are both promoted through different online and offline platforms and more importantly, they showcase the efforts of the two states in creating a holistic strategy (i.e. government, industry, civil society, academia) to ensure a secure and resilient cyberspace necessary for sustain economic growth. Brunei's digital diplomacy is also oriented towards enhancing economic growth as however, the state is still in the process of developing the essential components necessary for a robust digital environment that can attract foreign companies. The key barriers for Brunei include strong state regulation against cyber engagement, lack of a dedicated cyber strategy, imbalanced of collaboration between stakeholders in cybersecurity among others.

Small states have been successful in using networked-enabled diplomacy to advance norms, strengthen international cooperation, and enhance economic growth. Diplomacy is a principal foreign policy tool of small states because they are inherently constrained from employing other more intrusive measures such as military action. The use of cyber capabilities is therefore crucial to supplementing diplomatic efforts of New Zealand, Singapore, and Brunei because of two reasons. The first is that cyber capabilities enable small states to enlarge their diplomacy engagement through cyberspace limiting the resources necessary to extend their influence.  Since the barriers to entry are lower in cyberspace (Sheldon, 2013), systematically advancing ideas and promoting initiatives will not require substantial resources that small states might not have. The second is that since diplomacy is essentially about negotiation and communication (Diez, et al., 2011, pp. 33-35), the rapid and timely diffusion of essential information facilitated by cyberspace can be instrumental in advancing interests during negotiations.

*Covert action*

The second adjunct function is covert action or a state activity that pertains to "the effort of one government to influence politics, opinions, and events in another state through means which are not attributable to the sponsoring state" (Anderson, 1998, p. 423). This function typically includes measures that have been prominently discussed such as sabotage and subversion (Denning, 1999; Rattray, 2001; Rid, 2012) however, hacktivism can also be conceptualised as part of this function since all these measures have the same objective: signalling foreign policy preferences.  Covert action is a useful function of cyber capabilities particularly when states use these capabilities for covert communications, specifically signalling resolve towards a specific issue. Resolve is communicated credibly through costly signals such as military troop deployments (sinking costs), deliberately increasing risks such as by escalating conflicts (raising risks) and/or engaging political dynamics to reduce future flexibility such as public statements of intent by state leaders that affect national prestige (tying hands) (Fearon, 1997, p. 70; Carson and Yarhi-Milo, 2017, p. 128).

Carson and Yarhi-Milo (2017, pp. 125-126) contend that notwithstanding the secret nature of covert operations, states "find covert communication both intelligible (the basic intended message is understood by perceivers) and credible" because governments "have developed a basic interpretive framework that assigns meaning to observed covert behaviour." Based on this framework, the use of cyber capabilities for covert action is more sensible when the objective is to limit sinking costs, manage the risk of conflict escalation, and avoiding tying hands to manage audience cost because of the unique characteristics of cyber power. For instance, if the objective is to express disapproval over an adversary's activities in disputed territory, executing a DDoS attack to disrupt government operations is less costly than utilising military exercises. The risk of conflict escalation is also lesser with the use of cyber capabilities considering that even the most complex cyber weapons such as the Stuxnet instigate a conventional military response (O'Connell, 2012).

A prominent feature of covert action is its flexibility, providing states with more options to respond to emerging and current threats (Cormac, 2017, p. 15). Kello (2013) uses the term "special utility" to describe the unique ability of cyber operations to inflict calculated incidents: cyber weapons can inflict economic and political damage without resorting to violence. He postulates that cyber operations are strategic tools because these expand "the choice of actions and outcomes available to the strategic offense" (Kello, 2013, p. 26). Covert action provides states with alternative options that can generate specific foreign policy outcomes short of war but without causing any physical violence. Brantly (2016) makes a case for the utility of cyber capabilities as he classifies offensive cyber operations as part of a new means of executing covert operations that states can exploit to achieve foreign policy objectives. He contends that cyber capabilities are useful instruments because they can "alter a bargaining range between two states prior to engaging in or in attempting to avert an overt war" (Brantly, 2014, p. 466). Furthermore, what makes cyber operations advantageous for covert action is that it can provide alternative options for state sponsors of cyber intrusions. Since secrecy is integral to cyberspace, state sponsors have the option of exploiting this unique characteristic by claiming credit for the operation or denying responsibility and suffering the consequences if the incident is attributed to the sponsor (Poznansky and Perkosky, 2018). In both cases, it is unlikely for the targeted state to retaliate through military force thereby preventing any escalation or instability in the interaction of adversaries.

Both authors have presented some cases that illustrate the utility of cyber capabilities but the most compelling is *Operation Olympic Games*, a covert operation that can be classified as sabotage using cyber capabilities  (Kello, 2013, p. 26; Brantly, 2014, p. 479). The political objective of this operation was to prevent Iran from producing weapons-grade uranium as well as to convince Israel that an air strike was not a strong option (Farwell and Rohozinski, 2012, p. 111). The use of cyber capabilities was therefore a promising alternative because Israeli and U.S. intelligence agencies were confident that the cyber weapon could disrupt Iran's uranium enrichment programme temporarily while avoiding retaliation. Despite the limited impact on Iran's ability to enrich uranium, the operation still managed to "delay enrichment while averting a regional war" (Kello, 2013, p. 26).

Another less aggressive measure within covert action is hacktivism or the convergence of hacking and activism to advance a political agenda (Goode, 2015). This involves low-risk activities that aim to irritate targeted states through various methods such as website defacements, denial of service attacks, spread of malicious software, computer break-ins, and other forms of online protest (Denning, 2001, pp. 263-280). This tactic can be considered as part of covert action because it can also be used to repeatedly disrupt critical government services such as power grids and persuade hostile states to discuss contentious issues through diplomatic channels.

A well-known case that involves hacktivism is the distributed denial of service (DDoS) attacks by Russian-linked groups against Estonia in 2007. The cyber incident was a by-product of identity politics: the Estonian government downplayed the value of historical monuments relating to Soviet occupation while the ethnic Estonians and Russians highlighted the importance of preserving historical monuments because of its cultural and political significance (Russell, 2014, pp. 72-73). The tension between these groups intensified when the government relocated an important Bronze Solider monument, sparking violent demonstrations by ethnic Estonians and Russians and an official protest by the Russian government. Consequently, the political conflict inspired cyber intrusions that reflected the discontent of the Russian nationalists: shutdown of government websites, banks, telecommunications, media outlets, and name servers for several days.

This incident was executed through the use of botnets, a network of compromised machines that controlled by a "botmaster" to coordinate massive attacks against targeted systems (Reveron, 2012, p. 8; Tiirmaa-Klaar, et al., 2013, pp. 48-39). Using botnets to deny access to an adversary's networks and computer systems is an appropriate tactic of covert action because it makes attribution more arduous and retaliation through the use of military force unlikely.

Botnets are designed to be deceptive because they conceal the sponsor or coordinator of the attack by exploiting multiple computers and layers of servers that are exploited to carry out a DDoS attack for example (Tiirmaa-Klaar, et al., pp. 53-57). Moreover, attribution becomes more complicated if these computers and servers are located in multiple jurisdictions because of the difficulty in identifying, accessing, and actually investigating these machines (Clark and Landau, 2011). Retaliation through military force is unlikely because the use of botnets utilised for cyber intrusions do not inflict physical damage or harm therefore any kinetic military response is inappropriate. In this sense, targeted states will likely response through less intrusive foreign policy tools such as cyber intrusions or even negative sanctions. The incident involving Estonia raises two main implications. First, it compelled Estonia to rethink its foreign policy strategy towards Russia. This involved enhancing the scope of its defensive capabilities in coordination with NATO and its other allies. Second, the incident revealed the Estonia's vulnerabilities and forced it to strengthen its capacity for cyber operations and prevent another cyber blockade. This necessitated the development of an independent capability for cyber operations such as the Cyber Defence Unit of the Estonian Defence League as well as the establishment of the NATO CCDCOE in 2008.

*Network-enabled covert action and small states*

Conducting sabotage and subversion through cyber operations is a feasible foreign policy option for small states that have both the capacity and intention to carry out complex computer network operations against adversaries. In this regard, Singapore is the only state that has the potential to use cyber capabilities for this purpose because its existing military and technical capabilities and its intention to maintain an independent foreign policy provide the rationale for the aggressive use of cyber capabilities. Covert operations that use computer networks to destroy information systems or damage CNIs for instance require strong interagency collaboration particularly between intelligence agencies, military forces, and decision-makers to achieve the intended strategic objective. Singapore has the potential for these types of operations because of two reasons.

First, the state has existing capabilities for intelligence collection, special operations, and cyber operations, all essential components of covert operations. Singapore's participation in the Five Eyes intelligence network involved collecting information from undersea telecommunication cables, which indicates the states capacity for signals intelligence. (Dorling, 2013; Huang, 2013; Yu, 2013). In terms of special operations, Singapore's maintains the 1st Commando Battalion that is dedicated to missions such as infiltration, reconnaissance, and sabotage behind enemy lines (Huxely, 2000, p. 128). Lastly, the state's capacity to secure its government computer networks and CIIs was developed more than ten years ago but the more explicit demonstration of the state cyber capabilities started recently with the establishment of the Cyber Security Agency in 2016 and the formation of the Defence Cyber Organization in 2017 (Ng, 2017).

Second, in terms of implementation, the Singapore Ministry of Defence manages all these organisations and capabilities, which makes the integration of complex networked operations more feasible (Raska, 2016, pp. 152-153; Laksmana, 2017, p. 358). Moreover, the Cyber Security Agency, which is part of the Prime Minister's Office, overseas national cyber operations therefore the covert operation is properly aligned with the state's strategy and foreign policy direction. In terms of intention, Singapore prioritises foreign policy independence but it is difficult to develop a scenario where the state will use covert operations to influence an adversary's foreign policy. The state's strategy for survival is anchored on the pillars of diplomacy and deterrence (Matthews and Yan, 2007, p. 380) therefore covert action, which arguably involves more interference than economic sanctions and military exercises, would not be the most advantageous option for Singapore.

Employing cyber capabilities as part of covert action is not a realistic option for New Zealand and Brunei because both lack the capabilities and intention to execute such operations. New Zealand has the proven capacity for intelligence collection and for special operations however, there is no evidence to suggest that the state is interested in employing offensive cyber operations because the primary purpose in investing in cyber capabilities in both military and intelligence contexts is network defence (GCSB, 2014a; NDZF, 2016). More significantly, covert operations using cyber capabilities would be detrimental for New Zealand's foreign policy interests, considering its prevailing strategic culture that rejects intrusive cyber operations conducted by government agencies (Burton, 2013; Rogers, 2015). Brunei has modest capacity for intelligence and special operations but like New Zealand, there is also no evidence to suggest that its military and intelligence agencies have developed capabilities for offensive cyber operations. The state is still in the process of completing the basic elements necessary to defend its critical networks such as infrastructure, technical expertise, and responsible government agencies (Brunei Ministry of Defence, 2016). Brunei does not have the intention to carry out covert operations mainly because aggressive interventions contradicts the strategic culture of the state which favours a careful, non-aggressive approach in resolving foreign policy disputes.

Small states can also take advantage of hacktivist methods such as DDoS attacks because they are low impact and do not require extensive resources to implement. Based on Singapore's proven capacity for cyber operations and the direction of its foreign policy, it is the only state in the study that can potentially benefit from employing strategy. For instance, persistent website defacements can be a diplomatic tool to communicate a strong message or a "digital warning" regarding a contentious issue prior to any escalation or even military conflict. The prevalence of low level cyber incidents can either encourage an adversarial state to deescalate the tension by engaging in diplomatic talks or respond in kind through cyber skirmishes. Employing hacktivist methods to signal foreign policy preferences is a credible strategy for Singapore because its proven capacity to conduct cyber operations may compel other states to pursue a less aggressive strategy when dealing with the state. Moreover, Singapore's pursuit of an independent foreign policy by developing its military and intelligence capabilities reinforces its actions in cyberspace because it demonstrates consistency and resolve in defending its national interests.

These methods are less useful for New Zealand and Brunei because of their different strategic preferences as well as the direction of their foreign policies. New Zealand is known to have the capacity for cyber operations however, the state's strategic culture opposes aggression or the instigation of conflict in cyberspace thereby precluding the possibility of engaging in offensive cyber operations against adversaries. Cybersecurity is a core foreign policy issue for New Zealand, however the manner in which the state advances its interests in cyberspace is conducted through defensive (i.e. network defence and intelligence collection) and diplomatic (i.e. international organisations) strategies that complement its efforts to "gain greater autonomy in foreign policy" (Calintac, 2010, p. 334). Brunei on the other hand has yet to develop the capacity to conduct cyber operations but is unlikely to benefit from utilising hacktivist methods against adversaries as well. Cybersecurity is a national security issue in Brunei but the state's approach to securing cyberspace is directed by the Sultan. Brunei will not benefit from hacktivism because these methods contradict the state's strategic culture that is strictly conditioned by the Sultan's diplomatic approach to addressing geopolitical issues. Consequently, Brunei adheres to a "multifaceted" foreign policy strategy anchored on trade (i.e. oil and gas) and diplomacy (i.e. security alliances) to survive the geopolitical complexities of the Asia-Pacific Region (Chwee-Kuik and Welsh, 2005).

*Military action*

The third adjunct function is the use of cyber capabilities to amplify military action, particularly during war and coercion. These activities are treated distinctively in the chapter because they involve different methods: war requires direct physical violence or harm while coercion involves the threat of physical violence or harm to compel adversaries. The application of cyber capabilities to enhance military forces is the most prominent function articulated in the literature but most of these studies do not analyse cyber capabilities in the context of foreign policy (cf. Arquilla and Ronfeldt, 1993; Rattray, 2001; Libicki, 2007; Rid, 2013; Gray, 2013). This part draws substantially on the work of Borghard and Lonergan (2017) and Lindsay and Gartzke (2018) in defining the contribution of cyber capabilities as an adjunct function of military action. Cyber capabilities function as a force multiplier when employed in two core dimensions of military action: warfighting (attrition, denial, decapitation) and coercion (compellence and deterrence). In exploring these strategies, it is important to note that these discussions are mainly theoretical given that there are limited cases that involve the use of cyber capabilities in conventional military operations.

*Military action - warfighting*

War, according to Clausewitz (1832/2008, p. 13), is the "act of force to compel our enemy to do our will." Compelling adversaries necessitates different strategies such as attrition or protracted war against an adversary. The objective of this attrition is to gradually weaken the adversary's military force through small-scale and persistent strikes against their supply chain and logistics. Cyber operations can be effective tools for this strategy if these are utilised to destroy or corrupt "servers that handle military plans, air or ship tasking orders, or even defence developmental efforts" because the loss of these resources "can prevent certain actions from occurring at the time they are urgently needed" (Borghard and Lonergan, 2017, p. 474). This strategy is still hypothetical but is viable considering that military computer servers and databases have been prime targets of network intrusions since the transition of the Internet from military to civilian administration during the 1990s (Healey, 2014, 30-32; Naughton, 2016, pp. 11-12).

Another strategy in war is denial, which refers to the use of military force "to prevent the target from attaining its political objectives or territorial goals" (Pape, 1996, p. 13). Cyber operations can be a useful tool for denial when deployed to disable vital military systems such as integrated air defence systems, command and control platforms, and air traffic control systems prior to a conventional military attack (Borghard and Lonergan, 2017, p. 475). Targeting these important systems constitutes denial because it will convince the opponent that mounting a counteroffensive will be too costly to challenge. A concrete application of this strategy using cyber capabilities is *Operation Orchard*, when the Israeli Defence Force disabled Syria's air defence network to facilitate a successful air strike against a nuclear reactor. This strike successfully destroyed the facility and denied Syria the opportunity to further develop its nuclear programme. A more detailed discussion of this case in presented in Chapter 1.

Decapitation is a third strategy that would be effective when amplified by cyber operations. The objective of this strategy is to target the military leadership "because it is the only element of the enemy - whether a civilian at the seat of government or a general directing a fleet - that can make concessions" (Warden, 1992, p. 65). The logic behind this strategy is that once command and communications networks are destroyed, the link between military leadership and deployed units is severed thereby depriving enemy forces of clear central direction (Pape, 1996, p. 80). This strategy however is difficult to achieve using cyber capabilities considering that most states have redundant system designs that duplicate the critical components of a system to mitigate any disruption or failures in communications (Sterbenz, et al., 2010). In this sense, this hypothetical strategy can be effective when employed "at lower echelons of command, such as troops in the field, where there are typically fewer redundant systems, or against less-capable state adversaries" (Borghard and Lonergan, 2017, p. 476).

### *Network-enabled warfare and small states*

In terms of military action, the advantage in deploying cyber capabilities is that these enhance the capabilities of states for warfighting and coercion, however, this does not necessarily extend to states with weaker military forces. Cyber capabilities are potentially useful in complementing small states when the adversary's military strength is comparable or similar to the attacking state. Singapore is the only state in this study that can harness advantages of utilising cyber capabilities for attrition, denial, and decapitation in support of warfighting. The evidence such as Singapore's reputation for securing its CNIs and building strong cyber capabilities, has been discussed thoroughly in the previous chapters but the logic behind Singapore's case is that it has developed cyber capabilities to support its capable and cutting edge military force. Cyber capabilities can function as an effective force multiplier for small states only if there are technologically oriented military capabilities to begin with. This is not the case for New Zealand and Brunei.

New Zealand certainly has a capable military force but the trajectory of its modernisation is modest and defence-oriented therefore diminishing the necessity for investing in more sophisticated cyber capabilities for warfighting. Brunei is in the process of building a network-enabled military force but it is unclear if the state finds the strategic utility of developing cyber capabilities for warfare. While both states recognise the inevitability of cyber conflict, material and ideational constraints limit the opportunity for developing and utilising cyber capabilities as an effective enabler for fighting wars.

### *Military action - coercion*

Coercion in the context of military action is different from war. Coercion involves "the deliberate and purposive use of overt threats to influence another's strategic choices" (Freedman, 2003, p. 15). The potency of coercive strategies such as deterrence and compellence has been proven successful in conventional military operations however, the plausibility of these strategies when applied to cyberspace is still unclear (cf. Libicki, 2009; Lynn, 2010; Morgan, 2010; Lindsay, 2013, 2015; Denning, 2015; Kello, 2017; Nye 2017).[18] This discussion builds on the work Lindsay and Gartzke (2018) that explores assesses feasibility of coercive strategies when applied to cyberspace and the work of Poznansky and Perkosky (2018) that explores the politics of voluntary attribution for cyber operations. These studies suggest that deterrence and compellence are feasible depending on two variables: the type of cyber operation and method of communicating responsibility.

Lindsay and Gartzke (2018) contend that cyber capabilities are potentially useful when utilised to supplement military operations in the context of deterrence through detection, denial, and deception and in the area of compellence through latency and extortion. However, the success of coercive strategies depends on whether the attacker state can demonstrate resolve and credibility to its adversary (Carson and Yarhi-Milo 2017). Building on this, effective compellence and deterrence in cyberspace is therefore dependent a state's reputation for cyber operations. A concrete way of building a strong reputation for cyber operations is claim responsibility for cyber intrusions (Poznansky and Perkoskym 2018). Eliminating secrecy by claiming responsibility improves reputation of a state in two ways. First, credited intrusions can serve as costly signals by showcasing the attackers willingness to invest in considerable resources to compel the target to comply with its preferences. Second, credited intrusions can build prestige, which Poznansky and Perkosky (2018) define as "reputation for cyber power." These are are essential characteristics in implementing successful coercive strategies because states that develop "a reputation for cyber power may be able to persuade adversaries that their threats are credible" even if they do not specify the vector they plan to attack or the exploit they plan to employ if compliance is achieved (Poznansky and Perkosky, 2018). Deterrence by detection is possible through the implementation of extensive surveillance. A reputation for strong computer network exploitation improves general deterrence because this can discourage adversaries from conducting advance network intrusions that are essential for carrying out sophisticated and effective cyber operations (Buchanan, 2016, pp. 41-48). Furthermore, knowledge or fear of surveillance capabilities can also stimulate

[18] Deterrence is "the use of threats to dissuade an adversary from initiating an undesirable act." Compellence on the other hand, is a set of "strategies geared to coercing an adversary to do something or to stop doing something" (Freedman and Raghavan, 2008, pp. 217-218).

paranoia and force adversaries to focus on strengthening defensive rather than offensive capabilities.[19] Deterring adversaries by detection can be linked to the disclosures of Edward Snowden because it compromised the state secrets by revealing the cyber capabilities of the U.S. is and in turn reinforcing its reputation for cyber power. Lindsay and Gartzke (2018) argue that while the "leakage of top secret NSA documents has certainly compromised technical intelligence sources, it has also helped the U.S. to advertise the extent and technical skill of NSA penetration of the internet."

Deterrence by denial is feasible through the development of strong defensive capabilities. A robust defensive posture can be signalled through costly investments in the capabilities of intelligence agencies, law enforcement, regulatory agencies as well as the promotion of successful efforts in detecting and countering network intrusions (Lindsay and Gartzke, 2018). One example of signalling capabilities is the UK's announcement about its "active cyber-defence" strategy that involves "automated defences to offer protection from high-volume but relatively unsophisticated cyber-attacks" (Corera, 2016). Another example is Australia's recent declaration that it is establishing a new second Joint Cyber Security Centre. The mission of this new unit is to "provide up-to-date information about the nature and number of cyber threats, as well as help business and government better understand cyber risks and respond to them" (Tehan, 2017). Adversaries may challenge the credibility of these statements but the purpose behind signalling cyber capabilities is to communicate a level of readiness in countering cyber threats against the state.

Deterrence by deception is an existing strategy that has been applied by computer engineers to counter network attacks but is underrated in the context of cyber strategy. The objective of deception is to hide the real and to show the false (Whaley, 1982, p. 183). Applied to cyberspace, this strategy can be conceptualised into two tactics: deceptive hiding and deceptive showing. Deceptive hiding "conceals or obscures a thing's existence or its attributes in a way that intentionally misleads the target" while deceptive showing "makes something that does not exist appear as if it does by portraying one or more of its attributes" (Yuill, et al., 2006, p. 28). A concrete application of these tactics is the

[19] Buchanan (2016, pp. 111-112) suggests that purely defensive mechanisms exist. These include firewalls, anti-virus scanners, and software patches among others.

use of honeypot technologies to counter cyber threats. A honeypot "is a device—usually a computer server—that is purposely placed on a digital network in hopes that it will be compromised" (Bodmer et al., 2012, p. 115). These are primarily utilised for detection and information gathering against external threats and operate by misleading attackers into thinking that they are manipulating a legitimate sector of their target's network.

The case of *Cuckoo's Egg* illustrates one of the first effective applications of the honeypot. In 1986, a team of German hackers infiltrated several dozen computers at Lawrence Berkeley Laboratory network with the objective of stealing classified information regarding the U.S. Strategic Defence Initiative and satellites technology to be sold to the KGB (Healey, 2014, p. 29). An astronomer-turned-system administrator, Clifford Stoll managed to trace the hackers by devising bait that involved fictitious classified files with embedded alarms to determine who read them (Stoll, 2013, pp. 89-101). These deceptive tactics contribute to deterrence because they diminish the attacker's ability to intrude and manipulate target computer networks thereby making it exceptionally difficult to achieve their objectives.

### *Network-enabled deterrence and small states*

Besides warfare, small states can also benefit from coercive strategies that are augmented by cyber operations. It is possible for New Zealand and Singapore to benefit from using cyber operations for deterrence because these states have capabilities and interest to exploit cyberspace for detection, denial, and deception. There are four observable implications to support this assertion. First, both states are recognised to have sufficient military capabilities to defend their sovereignty. This factor is crucial because cyber operations only support military forces and independently coerce adversaries "to do something or to stop doing something" (Freedman and Raghavan, 2008, pp. 217-218). Second, in terms of detection, both states are acknowledged to have the operational capacity for computer network exploitation through New Zealand's official participation in the FVEY intelligence network and Singapore's unofficial contribution to the same network. The global surveillance reach of these states may influence other states in the Asia-Pacific to think twice before conducting network intrusions.

Third, in terms of denial, both states have invested in substantial resources to enhance the cyber capabilities of its security and military agencies. These cybersecurity efforts are not only well articulated in their respective cyber strategies but also communicated in various bilateral and multilateral meetings as well as through international institutions. Demonstrating a strong aptitude for cyber operations may discourage other states in the region from using computer network attacks against New Zealand and Singapore because of the difficulty and resources involved in attacking critical networks in these states.

Fourth, it is reasonable to assume that both states have the capacity for deception because of their strong interest in developing defensive measures against computer network attacks. It is difficult to determine if New Zealand and Singapore are actually using deception to deter attacks but the presence of active national computer security incident response teams and specialised programmes such as Project Cortex in New Zealand (Government Communications Security Bureau, 2014) and National Cybersecurity R&D Programme in Singapore (Cyber Security Agency, 2016) suggest a range of measures are being developed and utilised to defend critical networks.

Brunei's capacity for general deterrence is weak because of two reasons. The first is that the Royal Brunei Armed Forces is small and not known for force projection so it would be implausible for Brunei to compel other states even if these states have similar military strength. The second is that states are not aware of Brunei's cyber capabilities. The state has not released a clear cybersecurity strategy and has not created or designated any government agency to specifically counter cyber threats. Following these considerations, deterrence complimented by cyber capabilities is not a feasible strategy for Brunei.

Compellence by latency is a strategy that influences adversaries to mistrust their computer systems therefore weakening their cybersecurity posture.[20] The objective of this strategy is to make adversaries feel vulnerable by exploiting the period of uncertainty during the gap between network exploitation and attack (Lindsay and Gartzke, 2018). This gap typically occurs between a state's discovery of a vulnerability in the adversary's computer system and the adversary's

[20] Latency in computer studies "may be expressed as the time between initial infection and the time at which the degradation in system performance (due to widespread infection of executables) be comes unacceptable to the user. It may also depend on the delay between a virus initially infecting a program, and the commencement of malicious activity by the virus" (Ferbrache, 1992, p. 46).

awareness of the vulnerability (Smeets, 2017, pp. 8-11). In this context, escalation latency does not signal threat of harm but induces a "generalised paranoia" in targeted states due to the idea of compromised computer systems thereby persuading adversaries that resistance to cyber attacks is useless (Lindsay and Gartzke, 2018). Latency is potentially advantageous for powerful states that have formidable cyber capabilities that are projected in combination with conventional military capabilities. The contribution of latency therefore is its potential impact on the psychological dimension of compellence: making adversaries doubtful about the confidentiality, integrity, and availability of their computer systems.

Compellence by extortion leverages on the threat of disconnection from the Internet given the overpowering dependence of states on ICTs. The objective of this strategy follows the logic of blackmail: states need to comply with the demands of the coercing state or suffer the consequences of disconnection. The application of this strategy is limited for states but one hypothetical example cited Lindsay and Gartzke (2018) involves authoritarian states using threats of disconnection to intimidate the media, civil society and dissidents with the aim of forcing these groups to follow imposed restrictions. While this scenario may be considered as a strategy to control rather than compel, it still has a coercive component and demonstrates that cyber capabilities can potentially be used for extortion.

Brenner (2011, pp. 207-225) offers another hypothetical scenario of compellence by extortion. China blackmails a U.S. President by disabling a significant portion of the U.S. power grid (with generators monopolised by China) but only if the US recalls a carrier strike group heading to defend Taiwan. Even if Brenner (2011, p. 224) argues that "every aspect of the fictional scenario has already happened", this example is still implausible because the U.S. would consider this incident as an act of war and therefore use to conventional military force to retaliate against China. Compellence by extortion only make sense when weaker states are targeted such as China targeting Vietnam because of the South China Sea dispute or Russia targeting Ukraine as part of its coercive diplomacy (Valeriano and Maness, 2015a).

*Networked-enabled compellence and small states*

Like strategies for deterrence, the use of cyber capabilities to support compellence strategies such as latency and blackmail is only feasible if the state is capable of defending its national interests. Compellence however, is more difficult than deterrence because it necessitates stronger power projection since the objective is to change an adversary's existing action or behaviour. In this sense, Singapore is the only state in the study that can potentially take advantage of using cyber capabilities to compliment compellence strategies because it is recognised by the international community to have a strong and technologically oriented military force compared to most small states in the region. Compellence through latency and blackmail requires the right mix of capabilities, expertise, and military power to compel adversaries to change behaviour. Singapore has the strongest potential for specialised cyber operations because of the type of expertise, level of capabilities, and specific institutions that the state is building.[21]

New Zealand on the other hand, has the potential for deterrence but not compellence because of two reasons. First, while the state's military force is capable it is not configured for force projection.  Second, the most aggressive aspect of the state's cyber strategy is focused on building strong cyber defences to prevent or discourage adversaries for attacking the state. Since latency and blackmail require more intrusive and aggressive actions to coerce adversaries, these strategies contradict New Zealand's foreign policy interests that are anchored on diplomacy and engagements with international institutions. Brunei figures in the same predicament as New Zealand since its conventional military capabilities are very limited and it is still in the process of developing the capacity for cyber operations.

Cyber capabilities are new instruments for foreign policy that can transform interactions between states by uplifting less powerful states and levelling the playing field (Rustici, 2011). The analysis presented in the preceding sections contradicts this proposition. Despite the stated advantages of cyber capabilities, New Zealand, Singapore, and Brunei continue to rely on traditional

[21]The main research themes of Singapore's extensive National Cybersecurity R&D Programme focus on resilient systems, situation awareness and attack attribution, countering insider threats, threat detection and digital forensics among others (Singapore Prime Minister's Office, 2017). The Cyber Security Agency is assigned to manage cyber threat monitoring, cyber incident response, and cyber threat analysis while the Defence Cyber Organisation ensures the protection of defence and military networks in Singapore.

foreign policy instruments such as diplomacy and trade because these are still more effective in advancing their national interests in the Asia-Pacific Region. Cyber operations have limited use for small states and are not revolutionary foreign policy tools that enable the less powerful to change the dynamics of interstate conflict. Consistent with the preceding discussions, states can employ cyber capabilities as supplementary foreign policy tools of states. Since adjunct functions are useful in amplifying existing instruments, these can be incorporated in several categories within the foreign policy spectrum presented in Figure 3.

This section discussed the functionality of cyber capabilities, particularly the utility of these capabilities as adjunct functions to advance foreign policy interests. While the implementation of some strategies remains hypothetical, powerful states are in the forefront of developing new warfighting and coercive strategies for application in cyberspace, leaving less powerful states in a weaker position than originally postulated by the proponents of the cyber revolution (Lynn, 2010; Clarke and Knake, 2010; Kello, 2013, 2017). The next section discusses how cyber capabilities are assimilated within the broader spectrum of foreign policy instruments.

### *Cyber capabilities within the foreign policy spectrum*

Based on the preceding assessment, it is possible to locate cyber capabilities as part of the general foreign policy instruments used by small states. A comprehensive spectrum that includes all instruments does not exist because states can develop their own foreign policy tools depending of their resources, capabilities, strategic culture, and other variables (Smith, et al., 2016; Beach, 2010). The spectrum developed by Hill and Brighi (2016) is instructive for this purpose because it presents five consolidated categories of foreign policy tools organised in an escalation ladder. A modified version of this spectrum that compares traditional and networked-enabled foreign policy instruments of is presented in Table 5.

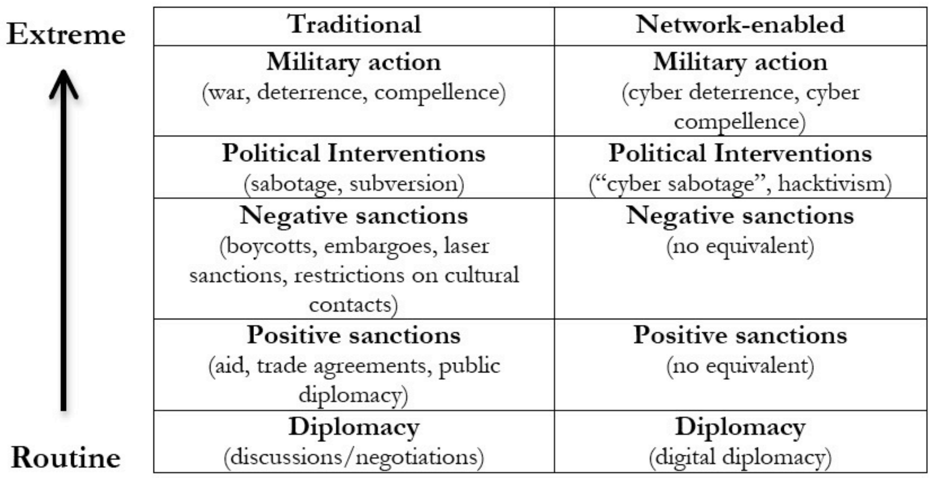
Following on this taxonomy, cyber capabilities can be integrated within the spectrum not as new forms of foreign policy tools, but as modified versions of existing instruments. Hacktivism is prominent example that illustrates this point because some academic scholars have argued that this tactic can be a distinct foreign policy instrument because of its uniqueness to the digital environment (cf. Denning, 2001; Nissenbaum, 2005; Solomon, 2017; Hare, 2017:

Lucas, 2017). Hacktivism is a favoured strategy by powerful states because they can execute large-scale disruption and denial of service attacks against other states with lower risk of attribution. However, belligerent protest activities are not new because similar tactics like civil disorder and demonstrations have long been employed by states as part of covert action to disrupt and destabilise adversaries (Shulsky and Schmitt, 2002, pp. 86-88). In this sense, hacktivism can be categorised as a measure within political intervention because of the covertness and intrusiveness involved in undertaking online political protests.

The use of networked technology to supplement positive and negative sanctions is already a common practice for states but the use of technology to supplement these functions does not translate to an active instrument that can advance foreign policy interests of states. More specifically, these functions involve passive measures that such as using encrypted online platforms for private communication between state leaders during embargoes or spying on a trading partner to improve a state's negotiating position in a trade agreement (Lindsay, 2015). For instance, China's cyber operations against the U.S. are predominantly focused on enhancing the state's economic competitiveness by stealing intellectual property of private companies. Indeed, China's systematic and extensive exploitation of computer networks to steal intellectual property was the main subject of the U.S.-China Cybersecurity Agreement that aimed to limit cases of cyber espionage between the two states (Harold, 2016; Heinl, 2017, pp. 132-133). While these types of cyber operations seem to have direct relevance to improving negative and positive sanctions, they are not unique networked-enabled tools and can be classified aa part of other tools such as intelligence collection or even covert action depending on the objective of the operation. Following this argument, the idea of "network-enabled sanctions" is not realistic because they cannot be employed as active instruments to shape foreign policy.

This section assessed the potential contribution of cyber capabilities when utilised to supplement traditional foreign policy instruments. Situating cyber capabilities within the foreign policy spectrum raises four key implications for the study of cyber strategy. First, cyber capabilities cannot supplement or enhance all traditional tools of foreign policy. This is evidence in the case of negative and positive sanctions because network technologies do not necessarily augment the implementation of sanctions such as foreign aid, embargoes, and trade agreements among other measures. Whereas these functions are staple foreign policy instruments that a useful to states, networked-enabled version of these functions do not contribute anything new to the foreign policy strategies of small states.

Second, cyber capabilities have limited utility because they can only supplement the foreign policy strengths of small states. Since diplomacy and covert action are the only two foreign policy functions that could be useful when supplemented by cyber capabilities, it would be advantageous for small states to focus their resources on these functions. Whereas it is sensible to assume that most small states are capable of managing in diplomatic relations, covert signalling as a form of covert action is more sophisticated and requires the state to develop the capability to interpret signals from adversaries and other states in the region. Third, small states will continue to strengthen their cyber capabilities even if the strategic utility of these capabilities is limited to specific functions. This assertion is based on literature that highlights the need for small states to explore all available strategies to survive in the international system (Handel, 1981; Hey, 2003). Since small states have no choice but to develop cyber capabilities for network defence, utilising them to advance foreign policy interests is a feasible strategy. Fourth, cyber capabilities would be useful for states if these were consider as enabler of various foreign policy instruments more than just military operations. Locating cyber capabilities as part of the wider foreign policy spectrum provides insight regarding the strategic utility of network technologies for small states. It is clear based on the preceding assessments that cyber capabilities are not revolutionary instruments because they are best utilised to strengthen existing foreign policy instruments employed by states. The point is crucial because it clarifies the hype from reality in cyber strategy.



| Extreme | Traditional | Network-enabled |
|---|---|---|
| | **Military action**<br>(war, deterrence, compellence) | **Military action**<br>(cyber deterrence, cyber compellence) |
| | **Political Interventions**<br>(sabotage, subversion) | **Political Interventions**<br>("cyber sabotage", hacktivism) |
| | **Negative sanctions**<br>(boycotts, embargoes, laser sanctions, restrictions on cultural contacts) | **Negative sanctions**<br>(no equivalent) |
| | **Positive sanctions**<br>(aid, trade agreements, public diplomacy) | **Positive sanctions**<br>(no equivalent) |
| Routine | **Diplomacy**<br>(discussions/negotiations) | **Diplomacy**<br>(digital diplomacy) |

Table 5: Traditional and networked-enabled foreign policy

## Conclusion

This chapter evaluated the utility of cyber capabilities as a foreign policy instrument for small states. It examined the adjunct functions of cyber capabilities and assessed the feasibility of these functions for the selected small states. The unique characteristics of cyber capabilities make it a practical tool for supplementing other foreign policy options. Although some scholars hypothesise about the independent or stand-alone potential of cyber capabilities, previous studies have not presented any compelling empirical evidence that verifies this assertion. In this context, it is more sensible to consider the adjunct function of cyber capabilities because cyber operations can amplify other foreign policy tools such as diplomacy, covert action, and military action.

Cyber diplomacy has become a standard practice for states to manage change through digital networks and virtual partnerships. Cyber operations can enhance diplomacy by enabling the participation of more stakeholders; allowing the rapid dissemination of information between states; and expediting the implementation of traditional diplomatic services to citizens and other governments. Cyber operations developed to supplement covert action are implemented to covey preferences regarding foreign policy issues to adversaries. Sabotage through cyber operations is a tactic within covert action. This involves the disruption of government services by disabling NCIs or destroying the arms production facility of a hostile state. Hacktivism or online political protests can also be conceptualised as part of covert action because it also disrupts government operations through various measures such as DDoS attacks to signal foreign policy preferences to the targeted state.

Cyber operations can supplement existing warfighting strategies of states through attrition by destroying servers and data centres; through denial by disabling vital military platforms and subsystems; and through decapitation by disconnecting deployed forces from command and control. Cyber coercion is difficult to achieve but theoretically possible. Adversaries are can be deterred through detection (extensive surveillance capabilities); denial (reputation for cyber operations); and deception (technical measures to discourage attacks). Cyber compellence is also feasible through latency (self-doubt) and blackmail (imposition of cost).

Cyber capabilities are not revolutionary foreign policy tools for small states. They are most useful when utilised for signalling foreign policy preferences towards adversaries. In this context, Singapore is most likely to benefit from utilising the full range network-enabled tools because of its capable military force and pre-emptive approach towards cyber threats. New Zealand can leverage some advantages from cyber capabilities by concentrating on cyber diplomacy and contributing to capacity development in the region. New Zealand is more likely to engage in cyber deterrence than compellence given its limited military capabilities and emphasis on defence. Brunei on the other hand, can only benefit from cyber diplomacy because of its limited resources, indefinite resolve, and competing views regarding the development and use cyber capabilities.

After explaining the rationale for developing cyber capabilities and the utility of these instruments, the final, concluding, chapter analyses the implications of the study by drawing out the main theoretical and policy contributions that make it useful for both academic and policy communities. Theoretical implications highlight the relevance of utilising existing theoretical frameworks in explaining and understanding cyber interactions. Policy implications emphasise the inadequacy of the ideas articulated by the cyber revolution thesis in assessing the impact of network technology on the strategy of small states. Chapter 7 also presents several areas for future research such as comparative studies of cyber strategies, the impact of the digital divide on cyber capabilities, and the role of non-state actors in cyber insecurity.

# Chapter 7
## Conclusion: Small States in Cyberspace

The idea that networked technologies can empower weaker states to "level the playing field" in strategic affairs is misleading. Small states have developed the capacity for cyber operations to defend their national interests from complex and persistent threats in cyberspace. While these capabilities can be used to advance foreign policy interests, they have not empowered weaker states to challenge or compete with more powerful states in the region. Despite the hype regarding the potential of networked technologies, the reality is that cyber capabilities are best utilised as enabling instruments that amplify the impact of traditional foreign policy tools.

While the most powerful states continue to developed innovative strategies that involve the use of cyber capabilities (Van Puyvelde and Brantly, 2017; Lindsay and Gartzke, 2018; Valeriano, et al., 2018a), small states have improved their capacity for cyber operations to enable them to cope with the impact of the uneven distribution of power in the region. In other words, structural conditions have compelled small states to develop cyber capabilities to support their self-reliance strategy for survival in the region. However, the strategic use of cyber capabilities is not straightforward. Small states must have a capable conventional military force as well as the intention to use cyber capabilities actively, as an instrument to advance foreign policy. Building on these conditions, this study contends small states such as Singapore would have the most success in using cyber capabilities for covert action, particularly signalling foreign policy preferences through cyberspace. Covert signalling has been an longstanding foreign policy practice between states but the use of networked technologies to convey preferences makes it more accessible and less risky for small states because of the unique characteristics of cyber power.

The findings of the study provided sensible and in-depth insights regarding the conditions that influence small states to develop cyber capabilities as well as the strong potential of cyber capabilities when utilised as an instrument to signal foreign policy preference to adversaries. However, making sense of strategic behaviour in cyberspace requires an answer to the quintessential strategic question: so what? (Gray, 2013, pp. 1-2). Based on this premise, this final chapter reflects on implications of the study by drawing out the main theoretical and policy contributions that make the prepositions and concepts discussed useful for both academic and policy communities.  The rest of this chapter proceeds in five parts. The first part summarises the main arguments of the study. The second discusses the relevance of existing theoretical frameworks in explaining state interactions in cyberspace. The third reconsiders the implications of the cyber revolution for the strategy of small states. The fourth reflects on the difficulties in implementing the study and the remedies applied to address these issues. The last section proposes future research themes in cybersecurity.

## Summary of the study

This study was designed to explore the rationale behind the development of cyber capabilities and to assess the utility of these capabilities as a foreign policy tool for small states. These objectives were pursued through the application of neoclassical realism as a theoretical framework to derive the conditions necessary for the use of cyber capabilities as a foreign policy instrument of small states, particularly New Zealand, Singapore and Brunei. This theoretical framework, as demonstrated in Chapter 3, was operationalized by deriving the conditions necessary for the development of cyber capabilities in small states. The distribution of power in the Asia-Pacific was identified as the primary condition that affects the foreign policy behaviour of small states, influencing these states to develop cyber capabilities. Strategic culture on the other hand, was recognised as a necessary secondary condition because while beliefs and practices cannot independently persuade states to harness the strategic value of ICTs, ideas are instrumental in filtering the responses of small states in adapting to the relative distribution of power.

Chapter 4 presented the case for the relative distribution of power as the primary condition that influences the foreign policy preferences of small states. Cyber conflicts do not occur in a vacuum and are manifestations of the geopolitical conflicts affecting states in the Asia-Pacific Region (Valeriano and Maness, 2015). The prevalence of territorial disputes, great power rivalry, and historical animosities are the main regional issues that motivate the continuous build-up of conventional military capabilities and consequently contribute to the disparity in military capabilities that favours the most powerful states. Since ICTs are instrumental in facilitating state interactions both in the physical and cyber domains, small states have developed cyber capabilities to enable them to respond more decisively to cyber conflicts provoked by the geopolitical tension in the region. The impact of the relative distribution of power on small states was analysed based on three observable implications: the response of small states to cyber conflict; the contribution of cyber capabilities in conventional military operations; and the connection between cyber capabilities and state power, focusing on the value of cyber power in the strategies of small states.

The analysis of the impact of uneven distribution of power on small states highlights two contributions to the literature on cybersecurity. The first is that the chapter validates the significance of existing geopolitical issues in instigating cyber conflicts in the Asia-Pacific. Cyberspace may be a new environment for state interaction but foreign policy behaviour is still driven by self-help and survival. Small states have therefore been compelled to develop cyber capabilities not because of its revolutionary potential but because of the need to adapt to a changing geopolitical environment. The second is that the chapter confirms the predominance of material resources in conditioning small states to develop cyber capabilities. Even if cyber conflict occurs in the digital domain, military forces and intelligence agencies still require physical resources such as computer servers, fibre optic cables, network nodes, and operators to execute cyber operations. Despite their inherent limitations, small states can certainly develop formidable cyber capabilities to coerce or challenge more powerful states but the utility of these capabilities will be limited. The most practical strategy for small states is to use cyber capabilities to amplify the foreign policy tools that have proven to be effective to address specific issues.

Chapter 5 explored the contribution of strategic culture as a necessary second condition that refines the foreign policy preferences of small states according to the beliefs and practices that are shaped by the geography and natural resources of small states. Strategic culture compliments the relative distribution of power as a primary condition since beliefs and practices function as a "transmission belt" that bridges systemic incentives and constraints on the one hand, and the foreign and security policies on the other (Lobell, et al., 2009, p. 4). The interaction of these variables is captured in the study by the concept of technology-oriented strategic culture or the preference of small states for using digital technologies to compensate for their material limitations in advancing foreign policy interests. The role of strategic culture in filtering strategic preferences of small states was established based on three observable implications: the contribution of strategic culture to the network readiness of states; the role of strategic culture in the development of cybersecurity strategies; and the influence of strategic culture in designating specific government agencies responsible for coordinating cybersecurity issues.

The integration of strategic culture as a supplement to the structural conditions postulated by the relative distribution of power makes three contributions to the literature on cybersecurity. First, the chapter affirms that culture is a relevant factor that affects military strategy and foreign policy. While the study treats culture as a secondary or "epiphenomenal" condition (Glenn, 2009, pp. 531-533), it still emphasises the crucial role of culture in defining the utility of cyber operations as well as producing a cyber strategy that is aligned with the foreign policy direction of small states. Second, consistent with the scope of this research, the chapter confirms that only limited generalisations can be drawn from evaluating the strategic culture of small states. Indeed, the contribution of the study focuses on the idea of a technology-oriented strategic culture, a concept that explicates the similarities between New Zealand and Singapore's efforts in building a network society and demonstrates the limitations of cultural generalisations in the case of Brunei. Third, the chapter illustrates that a theoretical framework that combines both systemic and state level constraints provides a more inclusive explanation regarding the foreign policy behaviour of small states. The explanations advanced in the study were not only able to elucidate the development of cyber capabilities but also interpret the intentions behind the cyber strategies of small states by examining their strategic beliefs and preferences.

Chapter 6 explored the utility of cyber capabilities and established that these capabilities had limited strategic value if utilised as a foreign policy instrument by small states. The chapter postulated that cyber operations would only be useful for small states under two conditions. The first condition is that small states need to have a capable technology-oriented military force to use cyber operations as part of its foreign policy arsenal. The second condition is that small states would benefit from using cyber operations only to pursue a limited objective: signalling foreign policy preferences. The literature on cybersecurity suggests that cyber capabilities are useful for both independent and adjunct functions of foreign policy however, no definitive argument or empirical evidence have been presented to validate the stand-alone potential of cyber capabilities as a foreign policy instrument. In this context, cyber capabilities are more useful as adjunct functions because they amplify rather than replace other tools in the foreign policy toolkit of states. In terms of foreign policy tools, the adjunct functions of cyber capabilities fall under three categories: diplomacy, covert action, and military action.

Employing cyber capabilities to amplify diplomatic measures has the most potential among the three functions because it allows small states to shape the foreign policy preferences of other states through negotiation and attraction rather than the use of military force. Cyber diplomacy has strengthened the diplomatic efforts of New Zealand and Singapore through norm promotion, international cooperation, and reinforcing economic growth. In contrast, cyber diplomacy has not been productive for Brunei because its strategic beliefs and practices inhibit full engagement with digital technologies. The feasibility of covert action for small states is not straightforward because it requires both capacity and intention to execute. Singapore is the only state in this study that can hypothetically benefit from engaging in cyber operations as part of covert action because of its preference for using advance military technology to pursue its foreign policy interests.

The same logic applies to cyber operations conducted to supplement warfare: capacity and intention are necessary for small states to take advantage of this function. Singapore is once again the only state in the study that can benefit from utilising cyber capabilities in support of warfighting because of its technology-oriented military force as well as its intention to maintain the technological edge over other states in the region. Cyber operations executed to amplify coercive strategies such as deterrence and compellence are also not realistic for small states with weak military forces. Cyber deterrence is feasible for both New Zealand and Singapore because these states are recognised to have the capability to defend their sovereignty and the operational capacity for computer network operations. Brunei may have the military capacity to protect its sovereignty, however it has yet to be recognised as a highly capable state in terms of cyber operations by the international community (Lewis and Neuneck, 2013;

Feakin, et al., 2015; International Telecommunications Union, 2017). Compellence using cyber operations is more difficult than deterrence because the objective of this strategy is to change an adversary's existing action or behaviour. Formidable military power projection is therefore vital for this strategy to succeed. This study argues that Singapore is the only state that can potentially harness the advantages of cyber compellence because it is recognised to have a highly capable and technology-oriented military force that is suitable for force projection. This function is not feasible for New Zealand because its military force is not designed for force projection and its cyber strategy is focused on building robust cyber defences. Brunei is in the same predicament as New Zealand since its conventional military capabilities are very limited and is still in the process of developing the capacity for cyber operations.

The assessment of cyber capabilities as a foreign policy instrument for small states makes two contributions to policy and strategy. First, the chapter distinguished "cyber hype" or perceived utility of cyber capabilities from "cyber reality" or the practical utility of cyber capabilities (Valeriano and Maness, 2015) by considering both material and ideational factors shaping the capabilities and intentions of small states. The reality that cyber capabilities have limited utility for small states is a useful premise to consider when developing policy responses to cyber incidents and implementing strategies that guide the use of cyber capabilities. Second, the chapter analysed the potential of cyber capabilities for signalling foreign policy preferences by small states. This function is vital for statecraft but it is not consequential enough to directly lead to the achievement of any strategic outcome. Cyber capabilities are more useful when they are utilised to support other foreign policy instruments. In this sense, it is necessary for small states to strengthen their diplomatic initiatives, military forces and intelligence capabilities if they intend to use cyber capabilities strategically.

## Implications for theory

The contribution of International Relations (IR) theories in exploring the impact of ICTs on international relations continues to be under-defined because of the lack of studies that theorise about cyber interactions. A key observation that captures this theoretical gap is that a substantial number of studies on cybersecurity are highly specific, policy-oriented, and provide limited insights regarding state response to cyber insecurity (Eriksson and Giacomello, 2006; Dunn Cavelty, 2007, 2010; Liff, 2012). Another argument is that existing IR theories have limited value in explaining state behaviour in cyberspace because the concepts and assumptions that underpin these theories are outdated (Valeriano and Maness, 2015, p. 54). This study has challenged these assessments by drawing on neoclassicial realism as a framework to understand the rationale for cyber capability development in small states as well as validating the continued relevance of conventional IR concepts and ideas to explain state interactions in cyberspace. This section presents three main theoretical implications that can be derived from this study.

### *Theory testing*

The first implication is the significance of theory testing. Assessing the suitability of existing IR theories has not been the norm in the literature on cybersecurity. The novelty and complexity of cyber phenomena, some scholars argue, render existing theoretical frameworks inadequate for explaining state behaviour in cyberspace (Choucri, 2012; Kello, 2017). This claim is misleading for two reasons. First, the proponents dismiss the potential of current IR theories without offering a systematic assessment of the strengths and limitations of these frameworks. In fact, the explanatory power of "old frameworks" has been substantiated by previous studies that highlight the importance of utilising current theoretical lenses in studying cybersecurity issues (e.g. Eriksson and Giacomello, 2006; Dunn Cavelty, 2007; Manjikian, 2010; Junio, 2013; Singh, 2013; Buchanan, 2016; Slayton, 2017).

Moreover, the actions of states in cyberspace are influenced by occurrences in the physical domain therefore IR theories remain sensible frames for systematic inquiry. Cyberspace may be a new environment for conflict and cooperation but the capabilities and intentions of states are still determined within the geographic dimensions of foreign policy: land, sea, air, and space (Gray, 1991, 1996, 2013). While ICTs can certainly amplify foreign policy interactions, outcomes are still determined in the physical domain. Existing IR theories are therefore still helpful in elucidating the complexities of online and offline foreign policy behaviour of states in the twenty first century.

Building on these arguments, this study has confirmed the significance of utilising IR theory in studying cyber phenomena by testing the explanatory power of neoclassical realism as a framework for analysing the cyber strategies of small states. While there are clear limitations to what the theory can explicate, it is instructive in developing an inclusive understanding of the conditions that influence the preferences of small states in using ICTs as a foreign policy tool. IR theories exist "to simplify a complex reality" (Mearsheimer and Walt, 2013, p. 431) therefore testing the potency of these frameworks in examining new occurrences such as cyber conflict is the necessary first step in advancing knowledge about state interactions in cyberspace.

### *Material and ideational factors*

The second implication is the relevance of both material and ideational factors in exploring state responses to cyber insecurity. Material factors such as economic resources and military capabilities are central to understanding the survival strategies of states because they determine the military capability and power. Since ICTs are more effective when used to amplify the capability and power of states, material considerations are integral to the development and use of cyber capabilities. On the other hand, ideational factors such as beliefs and practices are essential for understanding the motivation behind the foreign policy behaviour of states. ICTs were originally developed to accelerate the transactions as well as to enhance the diffusion of information. Strategic preferences or what states want to do with ICTs are influenced by ideas that are expressed through beliefs and practices of each state. These ideas affect the strategic direction and intention of states in advancing their foreign policy interests.

The study also has implications on the enduring debate regarding the primacy of either material or ideational factors in shaping security and policy strategies. The study postulates that material factors are more dominant than ideational factors in influencing the development of cyber capabilities as an instrument for small states within a specific region. This claim is anchored on three observations. First, states with extensive material resources have capable military forces and intelligence agencies that have the capacity to perform more sophisticated cyber operations against adversaries (Lindsay, 2013; Valeriano and Maness, 2015). Second, states with highest capacity for cyber operations are mostly located in the Asia-Pacific Region, where the relative distribution of power is determined by material more than ideational factors as proven by the build-up of conventional military forces that is driven by the struggle for territory and resources between rival states (Emmers, 2010; Bitzinger, 2010; Tan, 2014). Third, ideas are important in defining the purpose of ICTs but material resources such as networks and computers directly control execution cyber operations (Clarke and Knake, 2010; Craig and Valeriano, 2016). Furthermore, despite the pre-eminence of material factors, this study accentuates the need to consider the collaboration rather than the competition between material and ideational factors when probing into emerging areas of foreign policy interaction that remain understudied.

*Clausewitzian scepticism*

The third implication is the relevance of Clausewitzian scepticism in studying the impact of technology on the strategy of small states. Some scholars such as Kaldor (2005, 2010) and Kello (2013, 2017) argue that Clausewitzian thinking is outdated because the ideas are not configured to account for the complexities of war and conflict in the digital age. In terms of this study, the Clausewitzian school of war is sceptical of two major ideas: the transforming potential of cyber weapons (Rid, 2013; Valeriano and Maness, 2015) and the cyber revolution hypothesis (Lindsay, 2013; Gartzke, 2013). Adhering to the ideas of Clausewitz precludes the theoretical progression because it favours old models and discards the potential for a cyber theory that can accurately account for the new realities that are realised through ICTs (Kello, 2017, pp. 31, 55).

While revolutionist scholars make a strong case against scepticism, their arguments are more suitable when evaluating the impact of technology on the strategy of powerful states such as China, Russia, and U.S. (e.g. Rattray, 2001; Kello, 2017). This study finds that the cyber revolution thesis is not as potent as revolutionists contend, particularly when applied to the predicament of small states. Indeed, a key implication of this study is that Clausewitzian scepticism is instructive in exploring the strategy of small states in cyberspace. The first contribution of scepticism is the rejection of the concept of cyber war. The idea of war in cyberspace is invalid because it does not pass the Clausewitzian criteria of war: violent, instrumental, and political (Rid, 2013). Cyber incidents can be political and to a certain extent instrumental but cyber weapons are not violent. Computer network attacks that employ malicious software cannot directly inflict physical damage or harm against adversaries. This distinction matters because it clarifies the type of operations or actions states can undertake in cyberspace. Since war is not possible in cyberspace, states have recalibrated their strategies to determine how best to utilise cyber capabilities to advance their foreign policy interests.

A second contribution is that non-state actors are only secondary players in cyberspace. The primary role of states cyberspace has been discussed in several studies that are informed by Clausewitzian thinking (Betz and Stevens, 2011; Lindsay, 2013; Rid, 2013; Valeriano and Maness, 2015). While Clausewitz's strategic theory is not necessarily state-centric, he did recognise that "modern states had become capable of waging war on a major scale particularly through the comprehensive mobilisation of society and, therefore, had become dramatically more powerful strategic actors" (Vennesson, 2017, p. 13). Following this logic, states are the primary focus of this study because they have the capacity and resources to execute consequential cyber operations compared to non-state actors. More significantly, states are the only actors that have the "monopoly of the legitimate use of physical force" that allow them to respond to national security threats using military force (Weber cited in Jachtenfuchs, 2005, p. 37). The emphasis on states presented the opportunity to investigate a topic that is not typically considered in the debate on the primacy of actors in cyberspace: small states. Clausewitzian scepticism was therefore instrumental in defining the research puzzle that concentrates on the strategy of small states in cyberspace.

The third contribution is that Clausewitzian thinking exposed the limited strategic utility of cyber capabilities. The scepticism regarding the strategic potential of cyber capabilities can be summarised as three arguments articulated in the literature on cybersecurity. A key argument that has not been disputed even by revolutionists is the non-kinetic nature of cyber operations (Rid, 2013). This distinctive characteristic raises significant issues regarding the value of cyber capabilities as a strategic instrument considering that strategies that have been effective for coercion and warfare involve the use of physical force. Another argument is the inappropriateness of cyber capabilities as a stand-alone or independent foreign policy instrument. (Gray, 2013) This claim is validated by the fact that that all documented cyber operations to date were executed in concert with or as part of other foreign policy instruments such as diplomacy, covert action and military action. Chapter 6 presented provides a more comprehensive assessment of the functionality of cyber capabilities.

Yet another sceptical argument regarding the strategic potential of cyber capabilities is that it is unlikely to empower less powerful states in the international system (Valeriano et al., 2018, pp. 260-261). Sophisticated and instrumental cyber operations require "substantial time and institutional infrastructure" to implement against targets (Lindsay, 2013, 387). It is implausible for less powerful states with limited access to both material (infrastructure and funds) and ideational (technical knowledge and intelligence preparation) to weaponise malicious software and execute a cyber operation similar to *Olympic Games*. Following these assertions, this study confirmed that the utility of cyber capabilities is derived from its strength as an adjunct function to other foreign policy tools. The strategic utility of cyber capabilities further diminished when applied to the case of small states because not all of these states have the material resources as well as the inclination to use cyber capabilities for strategic purposes.

## Implications for policy

The policy discourse on national security and cyberspace was initially characterised by exaggerated and inaccurate declarations regarding the advantages of exploiting cyberspace as a new strategic domain for war and conflict (Dunn Cavelty, 2013, 2015; Lawson, 2013). The "revolutionary" potential of ICTs has shaped three main assumptions that have resonated within the foreign policy and military communities. The first assumption is that cyber capabilities empower weaker states because of the asymmetric advantages enabled by cyberspace (Clarke and Knake, 2010; Lynn, 2010; Obama, 2012; Alexander cited in Aftergood, 2013; Areng, 2014). The second assumption is that offensive operations are more potent compared to defensive operations in cyberspace (Hayden cited in Goodin, 2010; Clarke and Knake, 2010; Lynn, 2010; Clapper, 2013). The third assumption is that the strategy of deterrence is problematic when applied to cyberspace (Clarke and Knake, 2010; Hayden, 2011; Lynn, 2010; Stavridis, 2017).

These assumptions have been contested by recent studies that have reoriented the prevailing perceptions regarding state interactions in cyberspace and the functionality of cyber operations (Rid, 2013; Valeriano and Maness, 2015; Lindsay and Gartzke, 2015; Buchanan, 2016). This study has contributed to these debates by confirming the invalidity of some prevailing assumptions regarding cyberspace when applied to the case of small states. ICTs may be pervasive but how these strategic resources are harnessed is still dependent on material and ideational factors confronting states. This section presents three main policy implications that can be drawn from the study.

*Normality of cyber conflict*

The first implication is that low-level cyber conflict is likely to be an enduring feature of state interactions in the Asia-Pacific Region. Emerging trends such as the cloud services and Internet of Things will only increase the dependence of states on computer systems and networks thereby generating more economic opportunities but also creating more security vulnerabilities that can be exploited by adversaries. In this sense, there are two reasons why cyber conflict will become a normal part of state relations in the region. Firstly, as explicated in Chapter 4, cyber conflicts will become normal occurrences in the region because these incidents are a manifestation of geopolitical tension driven by political conflicts and rivalries between states. Employing computer network operations against adversaries have been advantageous for states because cyber skirmishes can be consequential without being lethal and escalatory (Kello, 2017). Even if cyber capabilities cannot generate the same outcomes as conventional military operations, they can still be used strategically to influence the behaviour of states involved in contentious geopolitical issues.

Secondly, cyber conflicts are likely to become part of normal state relations because of the utility of cyber capabilities in amplifying different instruments of foreign policy. As discussed in Chapter 6, cyber capabilities are useful for advancing foreign policy interests but the functionality of these capabilities depend on material resources as well as national preferences regarding the strategic use of cyber tools. Despite these constraints, states with various levels of capabilities have utilised cyber operations for influencing foreign trade negotiations (Lindsay, 2015); persuading regional institutions to engage in cyber capacity development (Heinl, 2013); disrupting the operations of transnational corporations (Knapp and Boulton, 2006); and facilitating espionage between competitors (Valeriano and Maness, 2015a). Whilst there are concrete regional efforts to mitigate cyber incidents, the uncertainty and insecurity regarding state behaviour in cyberspace will continue the prevalence of cyber conflicts in the region (Buchanan, 2016).

### *"Cyber evolution" for small states*

The second implication is the evolutionary rather than revolutionary impact ICTs on the strategy and foreign policies of small states in the region. Contrary to the assumptions anchored by the cyber revolution, this study has confirmed that the development of cyber capabilities by small states such as New Zealand and Singapore was a response to both external (relative distribution of power) and domestic (strategic culture) factors rather than an emulation of the capabilities of first movers such as China, Russia, and the U.S. Moreover, the build-up of cyber capabilities was executed gradually, within an extended time period as part of their respective strategies to adapt to the changing strategic environment and protect their foreign policy interests in cyberspace.

Based on this assessment, it is unlikely that small states can fully exploit the strategic advantages associated with cyber capabilities because of three reasons. First, small states are not first movers: they have developed cyber capabilities in response to the shifting strategic environment in the region. In this sense, cyber operations employed against more powerful states such as China, Russia or even North Korea will not translate to any concrete strategic advantage for small states because these states are early adopters of cyber capabilities and have the capacity to counter the most complex cyber intrusions. Whilst it is feasible for small states to employ cyber operations against other small states, it is likely that these actions will only produce strategic advantages if executed in support of conventional military operations. The closest example of this scenario is *Operation Orchard*, which was executed by the Israeli Defence Force against Syria in 2007 (see Chapter 1 for more details). Ultimately, as discussed in Chapter 6, small states would maximise the use of cyber capabilities as a foreign policy instrument to signal strategic preferences rather than a tool for coercion or warfare.

Second, small states may not necessarily favour the active use of cyber capabilities to pursue foreign policy objectives. The development and use of cyber capabilities is deliberate and based on the strategic preferences of states. Indeed, it is improbable for small states such as New Zealand to implement an aggressive cyber strategy even if it has the capacity to engage in sophisticated operations mainly because of its resolute stand against the militarisation of cyberspace. Intention and capability must be aligned if small states are to make use of ICTs as an instrument to advance foreign policy interests. Third, small states can only derive limited advantages from using cyber capabilities because they restrained from executing proactive and elaborate cyber operations against adversaries. The discussion in Chapter 4 highlighted that small states have limited material resources as well as conventional military forces relative to other states in the region. These limitations are crucial because even if cyber conflicts do not escalate into conventional military conflicts, it is likely that small states would still hesitate when operating against more powerful states because of the potential diplomatic and economic consequences that can be imposed once the cyber operation is attributed to the state.

### *Public-private partnerships in securing cyberspace*

The third implication is the importance of developing public-private partnerships in addressing cybersecurity issues. This study has established that small states have limited technical expertise, human resources, and infrastructure to develop the capacity to secure their respective national interests in cyberspace effectively. A key strategy for small states to compensate for these limitations is to build partnerships with the private sector as illustrated by the experiences of New Zealand and Singapore (see Chapter 4 for more details). The level of public-private collaboration is more institutionalised in Singapore than New Zealand because of its longstanding belief that building a technology-oriented state will enable it to maintain a strategic advantage over neighbouring states in the region (see Chapter 5 for more details). Indeed, the logic behind public-private partnerships is power sharing: the state has the authority and responsibility to protect NCIs and private companies have the expertise and resources to implement the state's mandate (Carr, 2016a). The need to develop public-private partnerships in cybersecurity raises two challenges for small states.

The first relates to the inclusion of public-private partnerships as a core element of cyber strategies. Small states will need to systematically integrate mechanisms for public-private partnerships in their cyber strategies if they intend to increase their capacity to counter cyber threats. This implies a more inclusive strategy that defines the role of various stakeholders aside from the state in securing networks and computer systems that are crucial for national security. Moreover, this inclusive strategy also addresses a broader range of cyber threats that affect different stakeholders (most notably the private sector) such as cybercrime and denial of service attacks. Given the pervasiveness of ICTs, highly networked small states would find it impracticable to develop and implement a robust cyber strategy without the expertise and resources provided by the private sector.

The second challenge pertains to mutual trust between the state and the private sector. The practice of information sharing is a core issue that continues to challenge the development of mutual trust between stakeholders in cybersecurity. The disclosure of sensitive information regarding security vulnerabilities as well as incidents of cyber intrusions is necessary for enhancing the capacity of stakeholders to respond to cyber threats (Dunn Cavelty and Suter, 2009). Information sharing has been a complicated task for states and private companies because of major trust issues that obstruct potential partnerships. For instance, private companies are reluctant to share information regarding cyber intrusions because of the possibility that competitors may learn about their vulnerabilities. States on the other hand are not inclined to disclose classified information because employees working with private companies do not necessarily have adequate security clearances (Carr, 2016a, pp. 58-59). While these challenges are complex and difficult to transcend, the strategies of New Zealand and Singapore demonstrate the feasibility of implementing mechanisms for public-private partnerships in managing cybersecurity issues.

## Research experience

Studying small state strategies in cyberspace was an immense challenge because of the ambiguity regarding the accessibility of relevant data and the appropriateness of existing theoretical frameworks in investigating an emerging field of inquiry. Despite the novelty of the topic, the main considerations in pursuing the study were the feasibility and validity of the research design and the core argument of the thesis. In this sense, this section discusses the main difficulties in implementing the study and the remedies applied to resolve these issues.

### *Setting parameters*

Establishing the parameters of the study was the first difficult challenge that needed to be resolved during the start of the research. The study is anchored in the field of International Relations but technical aspects of the subject matter inevitably required engagement with literature in other disciplines such as Computer Science (information security) and Sociology (technology and society). This was a key concern because it was not clear which concepts and ideas from these disciplines should be integrated to strengthen the substance of the study. This challenge was resolved in two steps.

Firstly, a literature review was implemented to assess the contribution of other disciplines in the area of cybersecurity. This involved a systematic reading of relevant journals, reports, and books in Computer Science and Sociology. Secondly, an evaluation was undertaken to determine which ideas (e.g. technological determinism, computer network exploitation, hacktivism) would be appropriate to improve the study. This entailed an evaluation of how previous studies in International Relations made use of concepts and ideas from other disciplines and applying them to the context of the study.

### *Case selection*

Selecting case studies was the second challenge that required a lot of time to resolve. The study focused on the Asia-Pacific Region because it is the most active area for cyber conflict however, the options were limited in terms of selecting cases to examine. For instance, Taiwan and South Korea were potential cases but due to their involvement in existing geopolitical rivalries, they were excluded from the study. A recent study by Valeriano and Maness (2015) has confirmed that cyber exchanges are more prominent among states engaged in geopolitical rivalries in the region therefore, selecting states that are part of these conflicts would prejudice the findings of the study. The challenge of selecting cases was resolved by clarifying the concept of smallness and selecting on the dependent variable (cyber capability).

The literature on small states presents a range of definitions; however, developing a specific definition that is informed by previous studies is essential for the effective implementation of the research. For instance, adopting an imprecise definition of smallness such as, smallness is what states make of it, would have been problematic since the study follows a most similar research design that necessitates specific criteria for selecting cases. It would also have been disadvantageous if a narrow definition was considered because the representativeness of the study would be affected. In terms of selection, the author purposely selected small states with existing cyber capabilities with the objective of uncovering the necessary conditions for cyber capabilities development. This "reverse engineering" was implemented to manage the lack of viable case studies as well as to come up with limited generalisations regarding the utility of cyber capabilities and strategy of small states in cyberspace. A more detailed explanation of the research design is presented in Chapter 1.

*Interviews*

Conducting interviews during fieldwork was the third challenge that required persistence and some creativity to overcome. The objective of the fieldwork in New Zealand and Singapore was to elicit information regarding the states' approach to cybersecurity from different stakeholders in government, private sector, and civil society. The difficulty in New Zealand was not the reluctance to share information but the limited number of people who had sufficient knowledge about the overall cyber strategy and specific measures being implemented by the state. The challenge in Singapore was the reluctance of people, in all sectors, to speak about the state's strategy to counter cyber threats or even the media report regarding cyber issues.

These barriers were addressed during the research process through advanced preparations and resilience during fieldwork. Advanced preparations involved developing contacts in New Zealand and Singapore during the first year of study, as soon as the research design and case studies were finalised. These contacts were strengthened by connecting with leading academics in institutions such as Victoria University Wellington in New Zealand and S. Rajaratnam School of International Studies in Singapore. An important part of advanced preparations was developing a list of interviewees, checking the feasibility of pursing these interviews, and following up with contacts right before fieldwork.

Resilience during fieldwork involved exhausting all efforts to contact relevant stakeholders for potential interviews and having an alternative collection plan just in case the interviews are cancelled. It was very difficult to secure interviews in Singapore so the author sent out numerous e-mails and talked to different people with hopes of increasing the chances for an interview. This technique was effective in securing interviews with civil society (media and academia) but not with the government and private sector. In the end, a combination of continued emails and help from contacts facilitated some interviews with government officials and private sector executives in Singapore. Meanwhile, as an alternative, the author continued data collection by consulting several public libraries that contained government documents and uncommon secondary materials. As a result, the combination of interviews and public documents produced sufficient data necessary for the systematic and detailed analysis of Singapore's cyber strategy.

## Directions for future research

Cybersecurity is not a new area of study; however, knowledge generated regarding cyber phenomena remains underdeveloped. This study focused on exploring the utility of cyber capabilities for small states with the objective of contributing to the limited understanding of the potential of ICTs for less powerful states in the region. While there are a number of emerging and unexplored themes in cybersecurity, this section presents three key areas for future research in studying cyber interactions.

The first research topic is comparing cyber strategies of states. Cyberspace has become a dynamic environment for competition and cooperation particularly for states that have strategic interests the region (Asia: The Cyber Security Battleground, 2013; Lindsay, 2015; Domingo, 2016). The assessment and comparison of cyber strategies is crucial because strategies provide some indication of the capabilities and intentions of states. Evaluating how states respond to cyber threats is a necessary task considering the complexity of cyber incidents as well as the lack of norms that guide state behaviour in cyberspace. Much like this study, a greater understanding of why states develop and implement specific strategies is central to managing cyber insecurity in the region because it can clarify misperceptions that contribute to the cybersecurity dilemma (Buchanan, 2016).

This task has not been straightforward because not all states in the region have cyber strategies or the states that actually have strategies are not inclined to disclose the information. Diplomatic initiatives and international institutions have alleviated the lack of transparency regarding intentions and capabilities but much progress still needs to be made if the objective is to mitigate cyber insecurity and strengthen current understanding about cyber interactions (Valeriano and Maness, 2015). In this sense, comparing the cybersecurity strategies of states is essential for building a stronger, more comprehensive understanding of cyber interactions in the region.

The second key topic is the impact of the digital divide on the cyber capabilities of states in the region. While highly networked states such as Singapore, New Zealand, and South Korea have taken the lead in upgrading their crucial information infrastructure and building cyber capabilities, a number of states such as Thailand, Cambodia, and the Philippines remain underdeveloped in terms of capabilities (Hanson et al., 2017). This disparity can be attributed to the digital divide or the "the gap in access to or use of ICT devices" (Ayanso, et al., 2010, p. 304) between states but the strategic implications of this imbalance has yet to be systematically explored in the region. The limited literature on the topic contends that developing states with relatively low capacity for cyber operations are in a weak position to counter computer network attacks however these studies have mostly focused on Georgia's case to support their claims (Ashmore, 2009; Gamreklidze, 2014).

Assessing the impact of the digital divide on cybersecurity is a fascinating research topic for the region because of two reasons. Firstly, a number of the states in the Asia-Pacific are developing economies that have limited network readiness, NCI and even less capacity for cybersecurity (Thomas, 2009). Although there has been a focused effort to improve network readiness and build capacity for cyber defence, the gap between advanced and developing economies cannot be reduced without any sustained cooperation between states in the region (Heinl, 2016). Secondly, while the limited capacity of developing states is considered as a disadvantage, it can also be transformed into an advantage. ICTs have a double-edged effect on states: the stronger dependence on technology, the higher probability of computer network attacks. Since developing states have low network readiness, it would be crucial to evaluate if this status can be utilised as a defensive measure against cyber intrusions. Cyber operations executed against developing states that have low network readiness can be an impractical strategy because the impact of the operation will be negligible and can be dismissed as a typical annoyance thereby missing the signal or message behind the action communicated by the responsible state.

The third salient research topic is evaluating the role of non-state actors in cyber insecurity. This study focused on states because they are the most powerful and influential actors in cyberspace. This assertion however does not preclude the participation of non-state actors in cyber interactions. The expanding literature on this topic suggests that non-state actors such as individual hackers, criminal organisations, cyber mercenaries, hacktivists, and patriotic hackers have been responsible for major cyber incidents (e.g. Denning, 2001; Mulvenon, 2009; Mumford, 2013; Bussolati, 2015; Karatzogianni, 2015; Maurer, 2018). Examples include espionage operations by China's patriotic hackers (Inkster, 2015, 67-70), disruption of Western media outlets by the Syrian Electronic Army (Valeriano and Maness, 2015, pp. 173-180) and more recently, the theft of nearly USD 1 billion from the Bangladesh Central Bank by hackers allegedly linked to North Korea (Maurer, 2018, p. 4). Even if these incidents are not as devastating as the Stuxnet attack against Iran or even the Shamoon attack against Saudi Aramco, the economic and social implications of these cyber incidents still contribute to insecurity between actors in cyberspace. There are two points that support this argument.

The first point is the difficulty of defending against cyber intrusions by non-state actors. Non-state actors conduct a substantial number of the intrusions against states however it has not been possible to eliminate these threats (Clapper, 2015, p. 2). The multiplicity of non-state actors that operate in cyberspace is so vast and unpredictable that states need to constantly develop new ways of protecting their networks and computer systems (Martin cited in Williams, 2017). This predicament therefore contributes to insecurity because it impossible for states to monitor the capabilities and assess the intentions of all non-state actors.

The second is the challenge of responding to non-state actors. It has been established that attribution is possible even for the most complex cyber intrusions by states (Rid and Buchanan, 2015) but another formidable challenge is responding to the malicious actions of non-state actors. Retaliating through cyber operations is an ineffective response against non-state actors because they are not fixed targets that are dependent on NCIs to survive (Dunn, 2006, p. 34). Punishing non-state actors through criminal prosecution is a viable response but it will take an extended amount of expertise, time, and resources particularly when cyber intrusions are multi-stage and cross-jurisdictional (Clark and Landau, 2006). In this sense, the source of insecurity for states is their inability to decisively respond to cyber threats by non-state actors, making this a valuable topic for future research in the field of cyber studies.

*   *   *

Networked technologies have transformed into tools that facilitate conflict and cooperation between states. While states are preoccupied with sustaining technological innovation, they have struggled to mitigate threats arising from increased dependence on technology.  Small states are in a particularly weak position to respond to these threats because of their high network readiness but weak capacity and resources to counter complex cyber intrusions. This predicament has compelled small states to develop cyber capabilities despite the prevailing ambiguity regarding the purpose and utility of these capabilities. This study has explored this puzzle by drawing on existing theoretical frameworks to understand why small states have developed cyber capabilities and by assessing the utility of cyber capabilities as a foreign policy instrument.

Small states can take advantage of cyber capabilities if they use them for diplomacy and covert action. Despite the emerging debates on the potential of cyber capabilities as a supplementary tool for warfare and coercion, these ideas are mostly applicable for powerful states with sufficient materials resources and strong military forces. Small states are not in the same category and would benefit from employing cyber operations if they are utilised to pursue a specific strategic: communicating foreign policy preferences. This assertion is not just based on a sceptical outlook towards cyber capabilities but a pragmatic assessment of the strategic realities confronting small states.

The emergence of more intrusive and sophisticated computer network operations in recent years has raised the level of aggression between states in cyberspace. It is therefore imperative for small states to make use of existing cyber capabilities combined with conventional foreign policy tools to strengthen their responses to aggression in cyberspace. While strategic thought on cyber power remains primitive, the ideas articulated in this study have hopefully distinguished reality over hype in exploring the strategy of small states in cyberspace.

# Appendix 1

## List of Interview Participants

### New Zealand

*Government*
Richard Elwin
Senior Analyst, Defence Policy Branch,
Ministry of Defence

Anthony Smith
Assessments Manager (Middle East and Asia), National Assessments Bureau,
Department of Prime Minister and Cabinet

Heather Ward
Policy Advisor, National Cyber Policy Office,
Department of Prime Minister and Cabinet

Andrew White
Analyst, International Security Division,
Ministry of Foreign Affairs and Trade

*Private Sector*
Laura Bell
Chief Executive, Safestack

David Eaton
Chief Technologist, Hewlett-Packard NZ

Anu Nayar
Partner – Risk Advisory, Deloitte New Zealand

*Civil society and academia*
Robert Ayson
Professor, Victoria University Wellintgon

Joe Burton
Lecturer, Victoria University Wellington

Barry Brailey
Director, New Zealand Internet Task Force

David Capie
Director, Centre for Strategic Studies,
Victoria University Wellington

Ben Creet
Senior Issues Advisor, InternetNZ

Martin Cocker
Executive Director, NetSafe

Neil Melhuish
Policy Advisor, NetSafe

Tom Pullar-Strecker
Senior Journalist, Dominion Post

Nathan Smith
Reporter, National Business Review

## Singapore

*Government*
Yu Han Wong
Director for Strategy
Cyber Security Agency
Prime Minister's Office/Ministry of Communications and Information

*Private Sector*
Anthony Lim
Senior Cybersecurity Advisor
Frost & Sullivan

Hock Beng Goh
Director and the Vice President for Asia Pacific
EB2BCOM

*Civil society and academia*
Benjamin Ang
Senior Fellow, Centre of Excellence for National Security
Rajaratnam School of International Studies

Alan Chong
Associate Professor
S. Rajaratnam School of International Studies

Lester Hio
Journalist, Singapore Press Holdings Ltd. Co

Kevin Kwang
Deputy Editor, Channel News Asia MediaCorp Pte Ltd.

Bernard Loo Fook Weng
Associate Professor
S. Rajaratnam School of International Studies

Tan See Seng
Associate Professor
S. Rajaratnam School of International Studies

Wu Shang-Su
Research Fellow, S. Rajaratnam School of International Studies

# Bibliography

Acharya, A. (2000). *Constructing a Security Community in Southeast Asia: ASEAN and the Problem of Regional Order*. London: Routledge.

Adams, J. (2001). Virtual Defense. *Foreign Affairs*, 80(3), 98-112. doi: 10.2307/ 20050154

Adams, K. R. (2003). Attack and Conquer? International Anarchy and the Offense-Defense- Deterrence Balance. *International Security,* 28 (3), 45-83. doi: 10.1162/ 016228803773100075

Adamsky, D. (2017). From Moscow with coercion: Russian Deterrence Theory and Strategic Culture, *Journal of Strategic Studies*, 41 (1-2), 1-28. doi: 10.1080/01402390.2017.1347872

Adamsky, D. (2010). *The Culture of Military Innovation*. California: Stanford University Press.

Adee, S. (2008, May). The Hunt for the Kill Switch. *IEEE Spectrum* Retrieved from: https://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch

Aftergood, S. (2013, August). US Cyber Offense is "The Best in the World" Retrieved from http://fas.org/blogs/secrecy/2013/08/cyber-offense/

Akutsu, H. (2013, January). Previewing Park Geun-hye's Foreign Policy Agenda. *The Tokyo Foundation*. Retrieved from http://www.tokyofoundation.org/ en/articles/ 2013/previewing-park-geun-hye-foreign-policy

Allison, G. and Zelikow, P. (1999). *Essence of Decision: Explaining the Cuban Missile Crisis* (2nd Ed.). New York: Longman.

Alons, G. C. (2007). Predicting a State's Foreign Policy: State Preferences between Domestic and International Constraints. *Foreign Policy Analysis,* 3 (3), 211-232. doi: 10.1111/j.1743-8594.2007.00048.x

Alperovitch, D. (2011). *Revealed: Operation Shady RAT*. Santa Clara, CA: McAfee.

Anderson, E. E. (1998). The Security Dilemma and covert action: The Truman years*International Journal of Intelligence and CounterIntelligence* 11(4), 403-427. doi: 10.1080/08850609808435385

Anckar, C. (2008). On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research. *International Journal of Social Research Methodology,* 11 (5), 389–401. doi: 10.1080/ 13645570701401552

Ansip, A. (2017, 5 September). Speech by Vice-President Ansip at the CERT-EU 2017 Conference. Retrived from: https://ec.europa.eu/commission/ commissioners/ 2014-2019/ansip/announcements/speech-vice-president-ansip-cert-eu-2017- conference_en

Archer, C., Bailes, A. J. K., & Wivel, A. (Eds.). (2014). *Small States and International Security Europe and Beyond*. New York: Routledge.

Areng, L. (2014). *Lilliputian States in Digital Affairs and Cyber Security* (Tallinn Paper No. 4). Tallinn, Estonia: NATO CCDCOE.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is Coming! *Comparative Strategy*, 12(2), 141-165. doi: 10.1080/01495939308402915

ASEAN Regional Forum. (2012). ASEAN Regional Forum Reaffirming the Commitment to Fight Cyber Crime. Retrieved from: https://ccdcoe.org/asean-regional-forum-reaffirming-commitment-fight- cyber-crime.html

Ashmore, W. C. (2009) Impact of Alleged Russian Cyber Attacks *Baltic Security & Defence Review,* 11(1), 4-40. Retrived from: http://www.baltdefcol.org/files/files/ BSDR/BSDR_11_1.pdf

*Asia: The Cyber Security Battleground: Hearing before the Subcommittee on Asia and the Pacific of The Committee on Foreign Affairs, U.S. House of Representatives,* 113th Cong., 1 (2013). Retrieved from: https://docs.house.gov/meetings/FA/FA05/20130723/101186/HHRG-113-FA05-20130723-SD002.pdf

Ayanso, A., Cho, D.I., and Lertwachara, K. (2010). The Digital Divide: Global and Regional ICT Leaders and Followers. *Information Technology for Development*, 16(4), 304–319.

Ayson, R. (2016). *Asia's Security*. London: Palgrave Macmillan.

Ayson, R. (2012). Choosing Ahead of Time? Australia, New Zealand and the US-China Contest in Asia', *Contemporary Southeast Asia,* 34 (3), 338-364. doi: 10.1353/csa.2012.0025

Ayson, R. and Capie, D. (2012). Part of the Pivot? The Washington Declaration and US-NZ Relations. *Asia Pacific Bulletin* 172. Retrived from: https://www. eastwestcenter. org/node/33571

Baabie, E. (2011). *The Basics of Social Research 5th Edition* Belmont, CA : Wadsworth Cengage Learning.

Baker, S., Waterman, S. and Ivanov, G. (2010). *In the Crossfire: Critical Infrastructure in the Age of Cyber War.* Santa Clara, CA: McAfee.

Bailes, A. J. K., Thayer, B.A. & Thorhallsson, B. (2016) Alliance Theory and Alliance 'Shelter': The Complexities of Small State alliance Behaviour, *Third World Thematics* 1(1), 9-26. doi: 10.1080/23802014.2016.1189806

Ball, D. (2011). China's Cyber Warfare Capabilities. *Security Challenges*, 7(2), 81-103.

Ball, D. (2009). Arms Modernization in Asia. In A. H. T. Tan (Ed.), *The Global Arms Trade: A Handbook* (pp. 30-51). London: Routledge.

Ball, D. (2004). Intelligence collection operations and EEZs: The implications of new Technology, *Marine Policy,* 28 (1), 67–82. doi: 10.1016/j.marpol.2003.10.011

Ball, D. (1994). Arms and Affluence - Military Acquisitions in the Asia-Pacific Region *International Security*, 18(3), 78-112. doi: 10.2307 /2539206

Ball, D. (1993). Strategic Culture in the Asia Pacific Region, *Security Studies*, 3(1), 44-74. doi: 10.1080/09636419309347538

Baller, S., Dutta, S., & Lanvin, B. (2016). *The Global Information Technology Report 2016*. Geneva, Switzerland: World Economic Forum

Banchoff, T. (1999). *The German Problem Transformed: Institutions, Politics, and Foreign Policy, 1945-1995.* Ann Arbor, Michigan University of Michigan Press.

Banlaoi, R. (2009). Globalisation's Impact of Defence Industry in Southeast Asia In G. Till, E. Chew, and J. Ho (Eds.), *Globalization and Defence in the Asia-Pacific: Arms Across Asia* (pp. 194-218) London: Routledge.

Barnett, M. and Duvall, R. (2005) Power in International Politics *International Organization* 59 (1), 39-75. doi: 10.1017/S0020818305050010

Barston, R. P. (1973). *The Other Powers: Studies in the Foreign Policies of Small States* London: George Allen & Unwin.

Barzashka, I. (2013). Are Cyber-Weapons Effective? *RUSI Journal*, 158(2), 48-56. doi: 10.1080/03071847.2013.787735

Bauman, Z; Bigo, D., Esteves, P., Guild, E., Jabri, V. and Lyon, D. (2014). After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* 8(2), 121-144. doi: 10.1111/ips.12048

Beach, D. (2010). *Analyzing Foreign Policy*. London: Palgrave Macmillan.

Beasley, R. K., Kaarbo, J., Lantis, J. S., & Snarr, M. T. (Eds.). (2002). *Foreign Policy in Comparative Perspective: Domestic and International Influences on State Behavior, First Edition.* Washington D.C.: CQ Press.

Beeson, M. (2009). *Institutions of the Asia Pacific : ASEAN, APEC and beyond.* London: Routledge.

Belson, D. (2017). *Akami's State of the Internet Report* (First Quarter 2017). Cambridge, MA.: Akamai Technologies, Inc.

Bendrath, R. (2001). The Cyberwar Debate: Perception and Politics in the U.S. Critical Infrastructure Protection. *Information & Society: An International Journal*, 7, 80-103.

Bennett, A. (2004). Case Study Methods: Design, Use, and Comparative Advantages In D. F. Sprinz and Y. Wolinsky-Nahmias (Eds.), *Models, Numbers, and Cases: Methods for Studying International Relations* Michigan: University of Michigan Press.

Berger, T. U. (2003). *Cultures of Antimilitarism: National Security in Germany and Japan*. Baltimore, Maryland: Johns Hopkins University Press.

Besar, N. (2015). "Information Communication Technology, Identity, and Brunei Society: A Critical Literature Review" *Susurgalur: Jurnal Kajian Sejarah & Pendidikan Sejarah*. 3(2), 247-256.

Betts, R. K. (1994). Wealth Power, and Instability - East-Asia and the United States After the Cold War. *International Security*, 18(3), 34-77. doi: 10.2307/2539205

Betz, D. (2012). Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. *Journal of Strategic Studies*, 35(5), 689-711. doi: 10.1080/ 01402390.2012.706970

Betz, D., & Stevens, T. (2011). *Cyberspace and the State Towards a Strategy for Cyberpower*. London: International Institute of Strategic Studies.

Bercovitch, J., and Oishi, M. (2010). *International Conflict In The Asia-Pacific: Patterns, Consequences and Management.* New York Routledge.

Berg, B. L., & Lune, H. (2012). *Qualitative Research Methods for the Social Sciences, 8th Edition,* New York: Pearson Education.

Bezooijen, B. V. and Kramer, E. (2015). Mission Command in the Information Age: A Normal Accidents Perspective on Networked Military Operations *Journal of Strategic Studies* 38 (4), 445-466. doi: 10.1080/ 01402390.2013.844127

Biddle, S. and Oelrich, I. (2016). Future Warfare in the Western Pacific *International Security* 41(1), 7–48. doi:10.1162/ISEC_a_00249

Bigle, L. and Dumitras, T. (2012, October 16-18). *Before We Knew It An Empirical Study of Zero-Day Attacks In The Real World* Paper Presented at 2012 ACM Conference on Computer and Communications Security, Raleigh, North Carolina, United States. doi.10.1145/2382196.2382284

Bilbao-Osorio, B., Dutta, S., Lanvin, B. (Eds.) (2014). *The Global Information Technology Report 2014* Geneva, Switzerland: INSEAD and World Economic Forum.

Billo, C., & Chang, W. (2004). *Cyber Warfare An Analysis of The Means And Motivations of Selected Nation States*. Hanover, NH: Dartmouth College, Institute For Security Technology Studies.

Bitzinger, R. A. (Ed.). (2016). *Emerging Critical Technologies and Security in the Asia-Pacific* London Palgrave Macmillan.

Bitzinger, R. (2010). A New Arms Race? Explaining Recent Southeast Asian Military Acquisitions. *Contemporary Southeast Asia*, 32(1), 50-69. doi: 10.1355/cs32-1c

Bjola, C. and Holmes, M. (Eds.). (2015). *Digital Diplomacy: Theory and Practice New* York: Routledge.

Blank, S. (2008). Web War I: Is Europe's First Information War a New Kind of War? *Comparative Strategy* 27 (3), 227-247. doi: 10.1080/01402390. 2013.844127

Blomqvist, H.C. (1998). The Endogenous State of Brunei Darussalam: The Traditional Society versus Economic Development, *The Pacific Review,* 11(4), 541-555. doi: 10.1080/01495930802185312

Bloomfield, A. (2012). Time to Move On: Reconceptualizing the Strategic Culture Debate, *Contemporary Security Policy,* 33 (3), 437-461. doi: 10.1080/ 13523260.2012.727679

Boland, B., et al. (2015). *Southeast Asia: An Evolving Cyber Threat Landscape.* Milpitas, CA: FireEye, Inc.

Bolt, P. J. & Brenner, C. N. (2004). Information warfare across the Taiwan Strait *Journal of Contemporary China*, 13(38), 129-150. doi: 10.1080/ 1067056032000151373

Brinkmann, S. (2013). *Qualitative Interviewing*. Oxford: Oxford University Press.

Bodmer, S.M., Kilger, M., Carpenter, C. (2012). *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. New York: McGraw-Hill.

Boon, D. C. W. (2015). Singapore-US Defence Relations: Enhancing security, Benefiting Region. *The Straight Times.* Retrieved from: http://www.straitstimes.com/opinion/singapore-us-defence-relations-enhancing-security-benefiting-region

Booth, K., & Trood, R. (1999). *Strategic Cultures in the Asia-Pacific Region*. London: Palgrave Macmillan.

Booth, K., & Wheeler, N. (2013). *The Security Dilemma: Fear, Cooperation and Trust in World Politics.* London: Palgrave Macmillan.

Borghard, E. D. & Lonergan, S. L. (2017). The Logic of Coercion in Cyberspace. *Security Studies* 26 (3), 452-481. doi:

Bouma, G., Ling, R., and Pratt, D. (2010). *Religious Diversity in Southeast Asia and* *the Pacific*. Heidelberg: Springer.

Bowen. G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, 9 (2), 27-40. doi: 10.3316/QRJ0902027

Boyd, A., & Menting, M. (2015). *Global Cybersecurity Index and Cyberwellness Profiles*. Geneva, Switzerland: International Telecommunication Union.

Brantly, A. F. (2016). *The Decision to Attack*: *Military and Intelligence Cyber Decision-Making*. Athens, Georgia: University of Georgia Press.

Brantly, A. F. (2014). Cyber Actions by State Actors: Motivation and Utility. *International Journal of Intelligence and CounterIntelligence*, 27(3), 465-484. doi: 10.1080/08850607.2014.900291

Brawley, M. R. (2010). *Political Economy and Grand Strategy: A Neoclassical Realist View*. London: Routledge.

Brenner, J. (2011). *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin Press.

Breuning, M. (2007). *Foreign Policy Analysis: A Comparative Introduction*. London: Palgrave MacMillan.

Brewster, T. (2014). Trouble with Russia, trouble with the law: inside Europe's Digital Crime Unit. *The Guardian*. Retrieved from: https://www. theguardian. com/ technology/2014/apr/15/european-cyber-crime-unit-russia

Brighi, E. and Hill, C. (2016). Implementation and Behaviour In S. Smith, A. Hadfield, and T. Dunne (Eds.), *Foreign Policy: Theories, Actors, Cases* (3rd Ed.) (pp. 147-167). Oxford: Oxford University Press.

Brinkmann, S. (2013). *Qualitative Interviewing*. Oxford: Oxford University Press.

Brunatti, A. D. (2012). The Architecture of Community: Intelligence Community Management in Australia, Canada and New Zealand, *Public Policy and Administration*, 28 (2), 119–143. doi: 10.1177/0952076712458110

Brunei Information Department. (2017). Four Indonesians were expelled for supporting Terrorism. *Pelita Brunei*, Retrieved from http://www. pelitabrunei.gov.bn

Brunei Information Department. (2016). *Brunei Darussalam In Brief*. Brunei: Prime Mnister's Office. Retrieved from: http://www.information.gov.bn/ Theme/Home.aspx

Brunei Ministry of Communications. (2016). *National Digital Strategy 2016 – 2020: National ICT White Paper*. Brunei: Ministry of Communications.

Brunei Ministry of Communications. (2015). *National Manpower ICT Masterplan* Brunei: Ministry of Communications.

Brunei Ministry of Defence. (2016). The Defence Science and Technology Policy Framework Retrieved. from: http://www.mindef.gov.bn/SitePages/ Defence%20Science%20and%20Technology%20Policy%20Framework.aspx

Brunei Ministry of Defence. (2015). *Profile*. Retrieved from: http://www. mindef.gov.bn/SitePages/Cores%20Values.aspx

Brunei Ministry of Defence. (2011). *Defending the Nation's Sovereignty, Expanding Roles in Wider Horizons: Defence White Paper 2011*. Brunei: Ministry of Defence.

Brunei Ministry of Defence. (2004). *Defending the Nation's Sovereignty: Defence White Paper 2004*. Brunei: Ministry of Defence.

Brunei Ministry of Foreign Affairs and Trade. (2006). *Brunei Darussalam & The People's Republic of China 1991-2006*. Brunei: Foreign Affairs and Trade.

Brunei Prime Minister's Office (2016). "Security and Enforcement" Retrieved from: http://www.pmo.gov.bn/about-pmo/division/security-and-enforcement

Brunei Prime Minister's Office (2015). *Digital Government Strategy 2015 – 2020* Brunei: Prime Minister's Office.

Brunei Prime Minister's Office. (2014). Warning for those who 'mock' Syariah law. Retrieved from: http://www.pmo.gov.bn/Lists/2014%20PMO %20News/NewDispForm.aspx?ID=46&ContentTypeId=0x0100641EF4 6C7802DC4F82AE04FB6244B1A2

Brunei Prime Minister's Office (2012). Brunei International Security Department Retrieved from: http://www.kdn.gov.bn/isd/index.htm

Brunei Prime Minister's Office (n.d.). Brunei International Security Department Retrieved from: http://www.kdn.gov.bn/isd/index.htm

Bryman, Alan (2012). *Social Research Methods, 4th Edition.* Oxford: Oxford University Press.

Buchanan, B. (2016). *The Cybersecurity Dilemma*. London: Hurst & Co. Ltd.

Bumgarner, J. and Bord, S. (2009). *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008,* Norwich, Vermont: U.S. Cyber Consequences Unit.

Burton, J. (2013). Small States and Cyber Security: The Case of New Zealand. *Political Science,* 65(2), 216-238. doi:

Burham, P., Gilland, K., Grant, W., and Henry-Layton, Z. (2008). *Research Methods in Politics SecondEdition*. Basingstoke: Palgrave Macmillan.

Bussolati, N.(2015). The Rise of Non-State Actors in Cyberwarfare In J. D. Ohlin, K. Govern and, C. Finkelstein (Eds.), *Cyberwar* Oxford: Oxford University Press.

Butcher, A. (2012). Students, Soliders, Sports, Sheep and the Silver-Screen: New Zealand's Soft Power in ASEAN and Southeast Asia. *Contemporary Southeast Asia,* 34(2), 249-273. doi: 10.1355/cs34-2e

Buzan, B. (1987). *An Introduction to Strategic Studies: Military Technology and International Relations*. New York St. Martin's Press.

Cammack, P., Pool, David and Tordoff, William (Ed.). (1988 ). *Third World Politics: A Comparative Introduction* London: Palgrave MacMillan.

Carlsnaes, W. (2016). Actors, Structures, and Foreign Policy Analysis In S. Smith, A. Hadfield, and T. Dunne (Eds.), *Foreign Policy: Theories, Actors, Cases* (3rd Ed.) (pp. 113-129). Oxford: Oxford University Press.

Carson, A. (2016). Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War. *International Organization,* 70(1), 103–131.

Carson, A. & Yarhi-Milo, K. (2017). Covert Communication: The Intelligibility and Credibility of Signaling in Secret. *Security Studies,* 26(1), 124-15. doi: 10.1080/09636412.2017.1243921

Carr, M. (2017). Cyberspace and International Order In H. Suganami, M. Carr, and A. Humphreys (Eds.), *The Anarchical Society at 40* (pp. 162-178). Oxford: Oxford University Press.

Carr, M. (2016). *US Power and the Internet in International Relations*. London: Palgrave Macmillan.

Carr, M. (2016a). Public–private partnerships in National Cyber-Security Strategies *Internstional Affairs* 92 (1), 43–62.

Castells, M. (2010). *The Rise of a Networked Society.* Malden, MA: Blackwell Publishers, Inc. (Original work published in 2000).

Castells, M. (May 9, 2001). The Network Society and Organizational Change. Retrieved from: http://globetrotter.berkeley.edu/people/ Castells/castellscon4.html

Castells, M. (2000). Toward a sociology of the network society. *Contemporary Sociology, 29*(5), 693–699. doi: 0.2307/2655234

Catalintac, A. L. (2010). Why New Zealand Took Itself out of ANZUS: Observing "Opposition for Autonomy" in Asymmetric Alliances *Foreign Policy Analysis,* 6 (4), 317–338. doi: 10.1111/j.1743-8594.2010.00115.x

Chachavalpongpun, P. (2013). Monarchies in Southeast Asia. *Kyoto Review of Southeast Asia,* March (Issue 13), pp. 1-6. Retrieved from: https://kyotoreview.org/issue-13-new/

Chan, S. (2013). Enduring Rivalries in Asia-Pacific. New York: Cambridge University Press.

Chaudhary, A.K.S.**,** Zaim, H. M.**,** Azizi, A.**,** Azmi, M. K. H. *Cyber Security for Power Systems.* Brunei National Energy Research Institute. Retrieved from: http://www.bneri.org.bn/ Shared%20Documents/Cyber%20security% 20final%20draft%20report.pdf

Cheng-Chwee, K. and Welsh, B. (2005). Brunei: Multifaceted Survival Strategies of a Small State, In William M. Carpenter and David G. Wiencek (Eds.), *Asian Security Handbook: Terrorism and the New Security Environment, 3rd ed.* (56-69) London & New York: M. E. Sharpe.

Cheng-Chwee, K. (2008). The Essence of Hedging: Malaysia and Singapore's Response to a Rising China. *Contemporary Southeast Asia, 30*(2), 159-185. doi: 10.1355/cs30-2a

Chong, A. (2014). Information Warfare? The Case for an Asian Perspective on Information Operations. *Armed Forces & Society, 40*(4), 599-624. doi: 10.1177/0095327x13483444

Chong, A. (2012). Singapore's Encounter with Information Warfare. In D. Ventre (Ed.), *Cyber Conflict Competing National Perspectives* (pp. 223-250). London, UK: ISTE, Ltd.

Chong, A. (2012). Singapore's Encounter with Information Warfare. In D. Ventre (Ed.), *Cyber Conflict Competing National Perspectives* (pp. 223-250). London, UK: ISTE, Ltd.

Chong, A. (2010). Small state soft power strategies: virtual enlargement in the cases of the Vatican City State and Singapore. *Cambridge Review of International Affairs* 23 (3)*,* 383-405. doi: 10.1080/09557571.2010.484048

Chong, A. (2006). Singapore's foreign policy beliefs as 'Abridged Realism': Pragmatic and Liberal Prefixes in the foreign policy thought of Rajaratnam, Lee, Koh, and Mahbubani *International Relations of the Asia-Pacific* 6 (2), 269–306. doi: 10.1093/irap/lci137

Choucri, N. (2012). *Cyberpolitics in International Relations*. Cambridge MA: MIT Press.

Christensen, T. J. (1999). China, the US-Japan alliance, and the security dilemma in East Asia. *International Security, 23*(4), 49-80. doi: 10.1162/isec.23.4.49

Clapper, J. R. (2015). Statement for the Record Worldwide Threat Assessment of the US Intelligence Community. Washington, D.C.: Senate Committee on Armed Services. Retrieved from: https://www.dni.gov/index.php/

Clapper, J. R. (2013). Statement for the Record Worldwide Threat Assessment of the US Intelligence Community. Washington, D.C.: Senate Committee on Armed Services. Retrieved from: https://www.dni.gov/index.php/

Clark, D. D. and Landau, S. (2011). Untangling Attribution. In Committee on Deterring Cyberattacks (Eds.), *Proceedings of a Workshop on Deterring Cyberattacks* (25-40). Washington DC: National Academies Press.

Clark, H. (2000). New Zealand Prime Minister Helen Clark: In Search of a Nation's Soul Time International Retrieved from: http://content.time.com/time/world/article/0,8599,2056080,00.html

Clarke, R., & Knake, Robert. (2010). *Cyberwar: The Next Threat to National Security and What to Do About It*. New York: HarperCollins Publishers.

Clausewitz, C. (2008). *On War*. (Michael Howard, Peter Paret, Trans.) Oxford: Oxford University Press. (Original work published in 1832).

Clemente, D. (2014). Cybersecurity In R. Dover, M. S. Goodman and C. Hillebrand (Eds.), *Routledge Companion to Intelligence Studies* (pp. 256-263) London: Routledge.

Coker, C. (2015). *The Improbable War: China, the United States and Logic of Great Power Conflict*. Oxford: Oxford University Press.

Collier, D. (1995). Translating Quantitative Methods for Qualitative Researchers: The Case of Selection Bias. *American Political Science Review* 89 (2), 461-466.

Collier, D. and Mahoney, J. (1996). Insights and Pitfalls: Selection Bias in Qualitative Research. *World Politics,* 49(1), 59–91. doi: 10.1353/wp.1996. 0023

Collins, A. (2003). *Security and Southeast Asia: Domestic, Regional, and Global Issues*. Boulder, CO: Lynne Reinner.

Collins, W., Lawrence, S.V., Rennack, D.E., and Theohary, C. A. (2015). *U.S.–China Cyber Agreement*. Washington D.C.: U.S. Congress Research Service.

Copeland, D. (2000). Review: The Constructivist Challenge to Structural Realism: A Review Essay. *International Security*, 25(2), 187-212. doi: 10.1162/016228800560499

Cormac, R. (2017). Disruption and Deniable interventionism: Explaining the Appeal of Covert Action and Special Forces in Contemporary British Policy. *International Relations,* 31(2), 169–191. doi: 10.1177/0047117816659532

Cornish, P., Livingstone, D., Clemente, D. and Yorke, C. (2010). *On Cyberwarfare: A Chatham House Report.* London: Royal Institute of International Affairs.

Corera, G. (2016, 13 September). UK moves to 'active cyber-defence' *BBC News* Retrieved from: http://www.bbc.co.uk/news/technology-37353835

Corwin, E. H. (2011). Deep Packet Inspection: Shaping the Internet and the Implications on Privacy and Security *Information Security Journal*: *A Global Perspective* 20 (6), 311-316. doi: 10.1080/19393555.2011.624162

Council of Europe. (n.d.). Budapest Convention and Related Standards. Retrieved from: https://www.coe.int/en/web/cybercrime/the-budapest-convention

Craig, A. and Valeriano, B. (2016, June). Conceptualising Cyber Arms Races, In N. Pissanidis, H. Rõigas, M. Veenendaal (Eds.), *Cyber Power.* Paper presented at the 8th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia (pp. 141-158). Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Crandall, M. (2014). Soft Security Threats and Small States: the Case of Estonia. *Defence Studies, 14*(1), 30-55. doi: 10.1080/14702436.2014.890334

Crandall, M., & Allan, C. (2015). Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms. *Contemporary Security Policy*, 36(2), 346-368. doi: 10.1080/13523260.2015.1061765

Croker, C. (2015). *The Improbable War: China, the United States and Logic of Great Power Conflict.* Oxford University Press, New York, USA

Croissant, A. and Loren.z, P. (2018). *Comparative Politics of Southeast Asia.* Switzerland: Springer International Publishing.

Crowards, T. (2002). Defining the category of 'small' states. *Journal of International Development*, 14(2), 143–179. doi: 10.1002/jid.860

Deibert, R., Manchanda, A., Rohozinski , R., Villeneuve, N. and Walton, G. (2009). *Tracking GhostNet: Investigating a Cyber Espionage Network.* Toronto: Citizen Lab, University of Toronto.

Denning, D. (2015). Rethinking the Cyber Domain and Deterrence. *Joint Forces Quarterly*, 77(2), 8-15. Retrieved from: http://ndupress.ndu.edu/Media/News/Article/581864/rethinking-the- cyber-domain-and-deterrence/

Denning, D. E. (2003). Cyber Security as an Emergent Infrastructure. In C. Irvine & H. Armstrong (Eds.), *Security Education and Critical Infrastructures* (pp. 1-2). Heidelberg: Springer.

Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy In J. Arquilla and D. F. Ronfeldt (Eds.), *Networks and Netwars : The Future of Terror, Crime, and Militancy* (pp. 239-288) Santa Monica, California: RAND Corporation.

Denning, D. E. (1999). *Information Security and Warfare.* New York Addison Wesley.

DeNardis, L. (2014). *The Global War for Internet Governance New Haven*, Connecticut: Yale University Press.

Desai, N. (Ed.). (2012). *India's Cyber Security Challenges*. New Dehli Institute for Defence Studies and Analyses.

Desch, M. (1998). Assessing the Importance of Ideas in Security Studies, *International Security* 23 (1), 141-170. doi: 10.1162/isec.23.1.141

Dibb, P. (1997) The Revolution in Military Affairs and Asian Security, *Survival* 39 (4), 93-116. doi: 10.1080/00396339708442946

Diez, T., Bode, I. & Da Costa, A. F. (2011). *Key Concepts in International Relations.* London: Sage Publications.

Ding, A. (2004). Taiwan: From Integrated Missile Defense to RMA? In E. Goldman & T. G. Mahnken (Eds.), The Information Revolution in Military Affairs in Asia. New York: Palgrave Macmillan.

Dian. M. (2015). The Pivot to Asia, Air-Sea Battle and contested commons in the Asia Pacific Region. *The Pacific Review* 28(2), 237-257. doi: 10.1080/09512748.2014.995124

Dion, D. (1998) Evidence and Inference in the Comparative Case Study *Comparative Politics* 30 (2), 127-145. doi: 10.2307/422284

Doeser, F. (2011). Domestic Politics and Foreign Policy Change in Small States The Fall of the Danish 'Footnote Policy'. *Conflict and Cooperation, 46*(2), 222-241. doi: 10.1177/0010836711406417

Domingo, F. (2016). Conquering a New Domain: Explaining Great Power Competition in Cyberspace. *Comparative Strategy* 35 (2), 154-168. doi: 10.1080/01495933.2016.1176467

Domingo, F. (2014). RMA and Small States. *Military and Strategic Affairs*, 6(3), 43-58. Retrieved from: http://www.inss.org.il/publication/the-rma-theory-and-small-states/?offset=2&posts=0&type=407

Domingo, F. (2014a). Conquering a New Domain: Explaining Great Power Competition in Cyberspace (unpublished MA thesis). University of Reading.

Dorling, P. (2013, November 25). Singapore, South Korea revealed as Five Eyes spying Partners. *The Sydney Morning Herald* Retrieved from: http://www.smh.com.au/technology/technology-news/singapore-south-korea-revealed-as-five-eyes-spying-partners-20131124-2y433.html

Dueck, C. (2006). *Reluctant Crusaders: Power, Culture, and Change in American Grand Strategy.* Princeton, N.J.: Princeton University Press.

Dueck, C. (2005). Realism, culture and grand strategy: Explaining America's peculiar path to world power. *Security Studies, 14*(2), 195-231. doi: 10.1080/09636410500232891

Dunn Cavelty, M. (2016) Cyber-security and Private Actors In R. Abrahamsen and A. Leander (Eds.), *Routledge Handbook of Private Security Studies* (pp. 89–99). New York: Routledge.

Dunn Cavelty, M. (2015). Cyber-security In A. Colins (Eds.), *Contemporary Security Studies 4th Edition* (pp. 401-415). Oxford: Oxford University Press.

Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, 20(3), 701-715. doi: 10.1007/s11948-014-9551-y.

Dunn Cavelty , M. (2014). *CyberSecurity in Switzerland.* Heidelberg: Springer.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review, 15*(1), 105-122. doi: 10.1111/misr.12023

Dunn Cavelty, M. (2008). Cyber-terror: Looming Threat or Phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology and Politics, 4*(1), 19-36. doi: 10.1300/J516v04n01_03

Dunn Cavelty, M. (2007). Is anything Ever New? – Exploring the Specifities of Security and Governance in the Information Age. In M. Dunn Cavelty & V. Mauer (Eds.), *Power and Security in the Information Age (pp. 19-44)* Aldershot, Hampshire: Ashgate Publishing Ltd.

Dunn Cavelty, M. (2006). Understanding Critical Information Infrastructures: An Elusive Quest In I. Abele-Wigert and M. Dunn (Eds.), *International CIIP Handbook 2006*. Center for Security Studies, ETH Zurich: Switzerland.

Dunn Cavelty, M. and Suter, M. (2009). Public-Private Partnerships are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection *International Journal of Critical Infrastructure Protection* 4 (2), 179-187.

Duraman, H. H. I. & Hashim, H. A. A. (1998). Brunei Darussalam: Developing Within Its Own Paradigm In D. Singh (Eds.), *Southeast Asian Affairs* (pp. 53-67). Singapore. Institute of Southeast Asian Studies.

Easley, L. (2014). Spying on Allies *Survival* 56 (4), 141-156.

East, M. (1973). Foreign Policy-making in Small States: Some theoretic observations based on a study of the Uganda ministry of foreign affairs *Policy Studies* 4 (4), 491–508. Retrived from:https://link.springer.com/article/10.1007%2FBF01728473

Easton, D. (1953). *The Political System: An Inquiry Into the State of Political Science.* New York: Alfred A. Knopf, Inc.

Easton, I., Stokes, M., Cooper, C. A., Chan, A. (2016). *Transformation of Taiwan's Reserve Force.* Santa Monica, CA.: RAND Corporation.

Ebert, H., & Maurer, T. (2013). Contested Cyberspace and Rising Powers. *Third World Quarterly, 34*(6), 1054-1074. doi: 10.1080/01436597.2013.802502

Eckielman, D. F. and Anderson. J. W. (2003). *New Media in the Muslim World.* Bloomington, IN: Indiana University Press.

Egberink, F., & van der Putten, F.-P. (2010). ASEAN and Strategic Rivalry among Great Powers. *Journal of Current Southeast Asian Affairs, 29*(3), 131-141. Retrived from: http://journals. sub.uni-hamburg.de/giga/jsaa/article/view/297

Elman, M. F. (1995). The Foreign Policies of Small States: Challenging Neorealism in Its Own Backyard. *British Journal of Political Science*, 25 (2), 171-217. doi: 10.1017/ S0007123400007146

Emmers, R. (2015). Security and Power Balancing: Singapore's Response to the US Rebalance to Asia In Tow, W. T. and Stuart, D. (Eds.), *The New US Strategy towards Asia* (pp. 115-128) London: Routledge.

Emmers, R. (2009). *Geopolitics and Maritime Territorial Disputes in East Asia*. London: Routledge.

Emmers, R. (2003). Cooperative Security and the Balance of Power in ASEAN and the ARF. London: Routledge.

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) Relevant Theory? *International Political Science Review,* 27(3), 221-224. doi: 10.1177/0192512106064462

Evans, P., Jacobson, Harold K., and Putnam, Robert D. (1993). *Double-Edged Diplomacy International Bargaining and Domestic Politics.* Califorina: University of California Press.

Farell, H. (2015). Promoting Norms for Cyberspace *Council of Foreign Relations* Retrieved from: https://www.cfr.org/sites/default/files/pdf/2015/03/Norms_ CyberBrief.pdf

Farrell, T. (2005). World Culture and Military Power *Security Studies* 14(3), 448-488.

Farrell, T., Osinga, F., and Teriff, T. (2010). A Transformation Gaps? Stanford, CA: Stanford University Press.

Farrell, T. and Teriff, T. (2002).*The Sources of Military Change: Culture, Politics, Technology*. Colorado, U.S.: Lynne Rienner Publishing.

Feakin, T., Woodall, J., and Nevill, L. (2016). *Cyber Maturity Index 2016*. Canberra: Australian Strategic Policy Institute.

Feakin, T., Woodall, J., and Nevill, L. (2015). *Cyber Maturity Index 2015*. Canberra: Australian Strategic Policy Institute.

Fearon, J. (1997). Signaling Foreign Policy Interests Tying Hands Versus Sinking Costs *Journal of Conflict Resolution,* 41 (1), 68-90. doi: 10.1177/0022002797041001004

Ferbrache, D. (1992). *A Pathology of Computer Viruses*. Heidelberg: Springer.

Finnemore, M. and Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organizations,* 52 (4), 887-917. doi: 10.1162/002081898550789Pub

Fleurant, A., Perlo-Freeman, S., Wezeman, P. D., & Wezeman, S. T. (2015). *Trends in international arms transfers*. Stockholm: Stockholm International Peace Research Institute.

Foulon, M. (2016). Neoclassical Realism: Challengers and Bridging Identities. *International Studies Review*, 18(2), 1-27. doi: 10.1111/misr.12255

Fravel, M. T. (2011). China's Strategy in the South China Sea. *Contemporary Southeast Asia,* 33 (3), 292–319. doi: 10.1355/cs33-3b

Freedman, L. (Eds.) (2003). *Strategic Coercion: Concepts and Cases.* Oxford: Oxford University Press.

Freedom House (2014). Freedom in the World: Brunei. Retrieved from: https://freedomhouse.org/report/freedom-world/2015/brunei

Freedman, L. & Raghavan, S. (2008) Coercion In Paul D. Williams (Eds.), *Security*

*Studies: An Introduction* (pp.216-227). London: Routledge.

Frieden, J., and Lake, D. A. (2005). International Relations as a Social Science: Rigor and Relevance. *Annals of the American Academy of Political and Social Science*, 600 (1), 136-156. doi: 10.1177/0002716205276732

Ganhdi, R., Sharma, A. Mahoney, W., Sousan, William, Zhu, Q., Laplante, P. (2011). Dimensions of Cyber Attacks: Social, Political, Economic, and Cultural *IEEE Technology and Society Magazine* 30(1), 28-38. doi: 10.1109/MTS.2011.940293

Gambino, L., Siddiqui, S., Walker, S., 2016 (30 December 2016). Obama expels 35 Russian diplomats in retaliation for US election hacking *Guardian* Retrieved from: https://www.theguardian.com/us-news/2016/ dec/ 29/barack-obama-sanctions-russia-election-hack

Gamreklidze, l. (2014). Cyber security in developing countries, a digital divide issue. *The Journal of International Communication*, 20(2), 200-217. doi: 10.1080/ 13216597.2014.954593

Garamone, J. (2012, January). Intelligence Chief Describes Complex Challenges. Retrieved from: http://archive.defense.gov/news/newsarticle. aspx?id=66999

Garnham, N. (2001). Contribution to a Political Economy of Mass-

Communication. In M.G. Durnham and D. M. Kellner (Eds.), *Media and Cultural Studies* (pp. 225-252). U.S.: Blackwell Publishing.

Gartzke, E. (2013). The Myth of Cyberwar Bringing War in Cyberspace Back Down to Earth. *International Security, 38*(2), 41-73. doi: 10.1162/ ISEC_a_00136

Gartzke, E., & Lindsay, J. R. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace *Security Studies*, 24(2), 316-348. doi: 10.1080/ 09636412.2015.1038188

Geers, K. (Eds.) (2015), *Cyber War in Perspective: Russian Aggression against Ukraine.* NATO CCD COE Publications: Tallinn.

Geers, K., et al. (2014) *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks.* Milpitas, CA: FireEye.

George, A. and Bennett, A. (2005) *Case Studies and Theory Development in the Social Sciences.* Cambridge, MA: Harvard University Press.

George, A. (1983). Crisis Prevention Reexamined In A. L. George (Ed.) *Managing U.S.- Soviet Rivalry: Problems of Crisis Prevention,* Boulder, CO: Westview Press.

Gerring, J. (2012). *Social Science Methodology: A Unified Framework.* Cambridge: Cambridge University Press.

Giles, K. (2016). *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power.* London: Royal Institute of International Affairs.

Giles, K. (2015). Russia and Its Neighbours: Old Attitudes, New Capabilities In K. Geers (Eds.), *Cyber War in Perspective: Russian Aggression against Ukraine* (pp. 19-28), NATO CCD COE Publications: Tallinn.

Girouard, N., Capozza, I., and Mazur. E. (2016).OECD Environmental Performance Reviews: New Zealand 2017. Paris, France: Organisation for Economic Co-operation and Development.

Glaser, C. L. (2015). A U.S.-China Grand Bargain? The Hard Choice between Military Competition and Accommodation. *International Security* 39(4), 49-90. doi: /10.1162/ISEC_a_00199

Glaser, C. L. and Kaufmann, C. (1998). What Is the Offense-Defense Balance and How Can We Measure It? *International Security* (22)4, 44-82. doi: 10.2307/2539240

Glenn, J. (2009). Realism versus Strategic Culture: Competition and Collaboration? *International Studies Review, 11*(3), 523-551. doi: 10.1111/j.1468-2486.2009.00872.x

Glenn, J. (Eds.) (2004) *Neorealism versus Strategic Culture.* Aldershot, Hampshire: Ashgate Publishing Limited.

Goetschel, L. (1999). Neutrality, a Really Dead Concept? *Conflict and Cooperation, 34*(2),114-139. doi: 10.1177/00108369921961807

Goertz, G. and Starr, H. (2002) *Necessary Conditions: Theory, Methodology, and Applications.* Lanham, Maryland: Rowman & Littlefield.

Goh, E. (2013). *The Struggle for Order: Hegemony, Hierarchy, and Transition in Post-Cold War East Asia.* Oxford: Oxford University Press.

Goh, E. (2007). Southeast Asian perspectives on the China challenge. *Journal of Strategic Studies, 30*(4-5), 809-832. doi: 10.1080/01402390701431915

Goh, E. (2006). Understading "hedging" in the Asia-Pacific *PACNET Newsletter*. Washington, DC: Pacific Forum CSIS.

Gold, M., & Wu, J. R. (2015). Taiwan seeks stronger cyber security ties with U.S. to counter China threat. Retrieved 10 April 2016, from https://www.reuters.com/article/us-taiwan-cybersecurity/taiwan-seeks-stronger-cyber-security-ties-with-u-s-to-counter-china-threat-idUSKBN0MQ11V20150330

Goldman, E. O. (2007). International Competition and Military Effectiveness: Naval Air Power, 1919–1945 In R. Brooks and E. A. Stanley (Eds.), *Creating Military Power: The Sources of Military Effectivenes*. Stanford, CA: Stanford University Press.

Goldman, E. (Ed.). (2004). *National Security in the Information Age*. London: Frank Cass Publishers.

Goldman, E. (2004). Introduction: Information Resources and Military Performance, *Journal of Strategic Studies*, 27 (2), 195-219. doi: 10.1080/0140239042000255896

Goldman, E. and Andres, R. (1999). Systemic Effects of Military Innovation and Diffusion. *Security Studies* 8 (4), 79-125.

Goldman, E. and Mahnken, T. (2004). *Information Revolution in Military Affairs in Asia.* London: Palgrave Macmillan.

Goldsmith, J.(2012). The Significance of Panetta's Cyber Speech and the Persistent Difficulty of Deterring Cyberattacks. Retrieved from:

https://www.lawfareblog. com/significance-panettas-cyber-speech-and-persistent-difficulty-deterring- cyberattacks

Goldsmith, J. and Williams, R.D. (2017). The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage. *Lawfare*, Retrieved from: https://www. lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage

Goldstein, L. (2015). *Meeting Halfway: How to Defuse the Emerging U.S.-China Rivalry.* Washington, D.C.: Georgetown University Press.

Gompert, D. C. and Binnendijk, H. (2016). *The Power to Coerce: Countering Adversaries without Going to War.* Santa Monica, CA.: RAND Corporation.

Gompert, D. C. and Libicki, M. (2015) Waging Cyber War the American Way *Survival*, 57(4), 7-28. doi: 10.1080/00396338.2015.1068551

Gompert and Libicki, M. (2014). Cyber Warfare and Sino-American Crisis Instability *Survival* 56 (4), 7-22. doi: 10.1080/00396338.2014.941543

Goode, L. (2015). Anonymous and the Political Ethos of Hacktivism. *Popular Communication,* 13(1), 74-86. doi: 10.1080/15405702.2014.978000

Goodin, D. (2010). Fog of cyberwar: Internet Always Favors the Offense *The Register* Retrieved from: https://www.theregister.co.uk/2010/07/29/internet_ warfare_keynote/

Gray, C. S. (2013). *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling.* Carlisle, PA: U.S. Army War College Press.

Gray, C. S. (2010). *The Strategy Bridge: Theory for Practice.* Oxford: Oxford University Press.

Gray, C.S. (2005). *Another Bloody Century: Future of Warfare.* London: Phoenix Press.

Gray, C. S. (1999). Strategic Culture as Context: The First Generation of Theory Strikes Back. *Review of International Studies*, 25 (1), 49-69. Retrieved from: https://www.jstor.org/stable/20097575?seq=1#page_scan_tab_contents

Gray, C.S. (1998). Explorations in Strategy—Strategic Utility of Special Operation Forces. Westport: Praeger Publishers.

Gray, C.S. (1991). Geography and Grand Strategy *Comparative Strategy,* 10 (4), 311-329. doi: 10.1080/01495939108402853

Gray, C.S. (1996) Rejoinder by Colin S. Gray, *Orbis*, 40 (2), 274-276. doi: 10.1016/S0030-4387(96)90065-4

Gray, C. S. (1981). National Style in Strategy: The American Example *International Security*, (6) 2, 21-47. doi: 10.2307/2538645

Gray, C. S. (1971). The Arms Race Phenomenon. *World Politics*, 24(1), 39-79. doi: 10.2307/2009706

Grauman, B. (2012). Cyber security: the vexed question of global rule. An independent report on cyber preparedness around the world. Brussels: Security and Defence Agenda, Brussels.

Grisby, A. (2017). The End of Cyber Norms. *Survival* 59(6), 109-122. doi: 10.1080/00396338.2017.1399730

Grisby, A. (2014). Coming Soon: Another Country to Ratify the Budapest Convention. *Council of Foreign Relations*, Retrieved from: https://www. cfr.org/blog/coming-soon-another-country-ratify-budapest-convention

Groll, E. (2017, 14 September). U.S. Navy Investigating if Destroyer Crash Was Caused by Cyberattack, Retrieved by:http://foreignpolicy.com/2017/09/

14/u-s-navy-investigating-if-destroyer-crash-was-caused-by-cyberattack/

Greenberg, A. (2017, 12 June ). Crash Override: The Malware That Took Down A Power Grid. Retrieved by: https://www.wired.com/story/crash-override-malware/

Gvalia, G., Siroky, D., Lebanidze, B., and Iashvili, Z. (2013). Thinking Outside the Bloc: Explaining the Foreign Policies of Small States. *Security Studies,* 22(1), 98-131. doi: 10.1080/09636412.2013.757463

Gvosdev, N. K. (2012). The Bear goes Digital: Russia and its Cyber Capabilities In D. Reveron, (Ed.). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (pp. 173-189). Washington D.C.: Georgetown University Press

Haacke, J. (2009). The ASEAN Regional Forum: from dialogue to practical security cooperation? *Cambridge Review of International Affairs, 22*(3), 427-449. doi: 10.1080/09557570903104057

Hager, N. (1996). *Secret Power: New Zealand's Role in the International Spy Network.* New Zealand: Craig Potton Publishing.

Haggard, S. and Lindsay, J. (2015). North Korea and the Sony Hack: Exporting Instability Through Cyberspace. *AsiaPacific Issues* No. 117.

Haglund, D. G. (2014). What Can Strategic Culture Contribute to Our Understanding of Security Policies in the Asia- Pacific Region? *Contemporary Security Policy*, 35(2), 310-328. doi: 10.1080/13523260.2014.927674

Haglund, D. (2011) 'Let's Call the Whole Thing Off'? Security Culture as Strategic Culture, *Contemporary Security Policy*, 32 (3), 494-516. doi: 10.1080/13523260.2011.623053

Hakmeh, J. (2017). Building a Stronger International Legal Framework on Cybercrime. *Royal Institute of International Affairs*, Retrieved from: https://www.chathamhouse.org/expert/ comment/building-stronger-international-legal-framework-cybercrime

Hare, F. B. (2017). Privateering in Cyberspace: Should Patriotic Hacking Be Promoted as National Policy?, *Asian Security* doi: 10.1080/14799855.2017.1414803

Hare, F. B. (2009). Private Sector Contributions to National Cyber Security: A Preliminary Analysis *Journal of Homeland Security and Emergency Management* 6(1), pp. 1-20. doi: 10.2202/1547-7355.1426

Harknett, R. J. and Steve, J. A. (2009). The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen. *Journal of Homeland Security and Emergency Management* 6 (1), 1-14. doi: 10.2202/1547-7355.1649

Harold, S. W. (2016). The U.S.-China Cyber Agreement: A Good First Step *The RAND Blog* Retrieved from: https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html

Haji Bakar, P. (2014, November 11). The Future, Our Responsibility Together, Speech by The Minister of Communications at the Launching Of National Broadband Policy & Cybersecurity Awareness Week 2014. Retrieved from: http://www.post.gov.bn/Lists/Speeches/

NewDispItem.aspx?ID=64&ContentTypeId=0x01009E303218B4B09449AE6D253837EBB2FC

Haji Mus, H. M. (2010). e-Government development In Brunei Darussalam [PowerPoint slides] Retrived from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_ Repository/Brunei_2010_unpan042980.pdf

Halpin E., Trevorrow, P., Webb, D., Wright, S. (2006). *Cyberwar, Netwar and the Revolution in Military Affairs*. London: Palgrave Macmillan.

Hammond, P. (2013, September). New cyber reserve unit created. Retrieved from: https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit

Handel, M. (1991). *Weak States in the International System* London: Frank Cass.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155-1175. doi: 10.1111/j.1468-2478.2009.00572.x

Harris, B. F. (2014) United States Strategic Culture and Asia-Pacific Security, *Contemporary Security Policy* 35(2), 290–309. doi: 10.1080/13523260.2014.928084

Harris, B. F. (2009). *America, Technology, and Strategic Culture: A Clausewitzian Assessment*. New York: Routledge.

Harrison, Lisa (2001) *Political Research: An Introduction* London: Routledge.

Hartfiel, R., & Job, B. L. (2007). Raising the risks of war: defence spending trends and competitive arms processes in East Asia. *Pacific Review, 20*(1), 1-22. doi: 10.1080/09512740601133138

Hass, P. M. (1992). Introduction: Epistemic Communities and International Policy Coordination. *International Organization* (46)1, 1–35.

Hayden, M. V. (2011). The Future of Things "Cyber" *Strategic Studies Quarterly* 5 (1), 3-7. Retrived from: http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-05_Issue-1/Hayden.pdf?ver=2017-01-23-115530-633

Hayat, H. (2018, 9 May). ISD detains local man with Islamic State link. *Borneo Bulletin*. Retrieved from: https://borneobulletin.com.bn/isd-details-local-man-with-islamic-state-link/

He, L. G. (2015). Cyberspace: What are the Prospects for the SAF? *Pointer: Journal of the Singapore Armed Forces* 41 (1), 58-70. Retrieved from: https://www.mindef.gov.sg/oms/imindef/publications/pointer/journals/2015/v41n1.html

Heywood, A. (2011). *Global Politics*. London: Palgrave Macmillan.

Healey, J. (Ed.). (2013). *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*. Virginia: Cyber Conflict Studies Association.

Heng. Y (2013). A Global City in an Age of Global Risks: Singapore's Evolving Discourse on Vulnerability *Contemporary Southeast Asia* 35 (3), 423-446. doi: 10.1355/cs-3e

Heilmann, D. (2015). After Indonesia's Ratification: The ASEAN Agreement on Transboundary Haze Pollution and Its Effectiveness As a Regional

Environmental Governance Tool *Journal of Current Southeast Asian Affairs*, 34 (3) 95–121.

Heinl, C. H. (2018). Can ASEAN Continue to Improve Cybersecurity in the Region and Beyond? *Council of Foreign Relations*, Retrieved from: https://www.cfr.org/blog/can-asean-continue-improve-cybersecurity-region-and-beyond

Heinl, C. H. (2017). New Trends in Chinese Foreign Policy: The Evolving Role of Cyber. *Asian Security*, 13(2), 132-147. doi: 10.1080/14799855.2017.1286160

Heinl, C. H. (2016). Regional Cybersecurity Policy Developments in Southeast Asia and the Wider Asia Pacific In S. Jayakumar *State, Society and National Security: Challenges and Opportunities in the 21st Century* (pp. 233-246) Singapore: World Scientific.

Heinl, C. H. (2013). Regional Cyber Security: Moving Towards a Resilient ASEAN Cyber Security Regime (Working Paper 263). Singapore: S. Rajaratnam School of International Studies Singapore.

Herman, M. G. and Preston, T. (2004). Presidential Leadership Styles and Foreign Policy Advisory Process In E. R. Wittkopf and J. M. McCormick (Eds.), *The Domestic Sources of American Foreign Policy: Insights and Evidence* (pp. 363-380) (4th Ed.). New York: Roman & Littlefield Publishers, Inc.

Herrera, G. L. (2006). *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*. Albany, New york: State University of New York Press.

Herrick, D. (2016). The Social Side of 'Cyber Power'? Social Media and Cyber Operations *Social Science Research Network* Retrieved from: https://papers.ssrn. com/sol3/papers.cfm?abstract_id=2803669

Hey, J. A. K. (Ed.). (2003). *Small States in World Politics*. Boulder, CO: Lynne Rienner Publishers.

Ng, E. H. (2017, March). Speech by Minister for Defence at the Committee of Supply Debate. Retrieved from: https://www.gov.sg/microsites/budget2017/press-room/news/content/speech-by-minister-for-defence-dr-ng-eng-hen-at-the-committee-of-supply-debate-2017

Herr, T. and Rosenzweig, P. (2016). Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model *Journal of National Law & Policy* 8 (2), 301-319. Retrieved from: http://jnslp.com/

Hill, C. (2003). *The Changing Politics of Foreign Policy*. London: Palgrave Macmillan.

Hill, C. and Brighi, E. (2016). Implementation and Behaviour. Steve Smith, et al. *Foreign Policy Theories, Actors and Cases* (pp. 147-166). Oxford: Oxford University Press.

Ho, S. H. (2009). Hegemony of an Idea (Discussion Paper n° 5 - Note de recherche n° 5). Retrieved from: http://www.irasec.com/ouvrage43

Hoffmann, A. L., Proferes, N. and Zimmer, M. (2018). "Making the world more open and connected": Mark Zuckerberg and the Discursive Construction of Facebook and its Users *New Media & Society* 20(1), 199–218.

Hoffman, W. and Levite, A. (2017). *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?* Washington D.C.: Carnegie Endowment for International Peace.

Holmes, M. (2015). Digital Diplomacy and International Change Management In C. Bjola and M. Holmes (Eds.), *Digital Diplomacy: Theory and Practice New* (pp. 13-32) York: Routledge.

Horowitz, M.C. (2010). *The Diffusion of Military Power: Causes and Consequences for International Politics*. New Jersey: Princeton University Press.

Horton, A.V.M. (1994). Review of Ideological Innovation Under Monarchy: Aspects of Legitimation Activity in Contemporary Brunei. *Modern Asian Studies* 2 (4). 891-893. doi: 10.1017/S0026749X00012579

Hoslag, J. (2015). *China's Coming War with Asia*. London: Polity Press.

Howard, P. (2015). *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up* London: Yale University Press.

Howard, P. (2010). The *Digital Origins of Dictatorship and Democracy*. Oxford: Oxford University Press.

Howard and Hussain (2013). Dem*ocracy's Fourth Wave? Digital Media and the Arab Spring*. Oxford: Oxford University Press.

Hudson, V. M. (2006). *Foreign Policy Analysis: Classic and Contemporary Theory*. New York: Rowman & Littlefield Publishers.

Hudson, V. M. (ed.) (1997) *Culture & Foreign Policy*. Boulder, CO: Lynne Rienner.

Hughes, C. W. (2009). Japan's response to China's rise: regional engagement, global containment, dangers of collision. *International Affairs, 85*(4), 837-856. doi: 10.1111/j.1468-2346.2009.00830.x

Hughes, R. (2010). A treaty for cyberspace. *International Affairs, 86*(2), 523-541. doi: 10.1111/j.1468-2346.2010.00894.x

Hughes, D., & Colarik, AM. (2016). Predicting the Proliferation of Cyber-Weapons into Small States. *Joint Force Quarterly*, 83 (4), 19-26.

Hura, M. , McLeod, G W., Larson, E V., et al. (2000). *Interoperability: A Continuing Challenge in Coalition Air Operations Santa Monica*. CA: RAND Corporation.

Hurel, L. M. & Lobato, L. C. (2018). Unpacking cyber Norms: Private Companies as Norm Entrepreneurs, *Journal of Cyber Policy* 3(1) 61-76. doi: 10.1080/ 23738871. 2018.1467942

Huxley, T. (2006). Singapore's Strategic Outloook and Defence Policy In J. C. Liow and R. Emmers (Eds.), *Order and Security in Southeast Asia* London: Routledge.

Huxley, T. (2004). Singapore and the Revolution in Military Affairs In E. Goldman and T. Mahnken, *The Information Revolution in Military Affairs in Asia* (pp. 185-208) London: Palgrave Macmillan.

Huxley, T. (2000). *Defending the Lion City*. Sydney: Allen & Unwin.

Hwang, J. J. (2012). China's Cyber Warfare: The Strategic Value of Cyberspace and the Legacy of People's War (unpublished doctoral thesis). University of Newcastle.

Ingebritsen C., Newman, I. & Sieglinde, G. (2006). *Small States in International Relations*. Seattle, WA.: University of Washington Press.

Inbar, E., & Sheffer, G. (Eds.). (1997). *The National Security of Small States in a Changing World.* London: Frank Cass.

Inserra, D. and Rosenzweig, P. (2014) Cybersecurity Information Sharing: One

Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace. *The Heritage Foundation,* Retrieved from: http://report.heritage.org/bg2899

International of Institute of Strategic Studies (2015). *Military Balance 2015.* London: Routledge.

Inkster, N. (2016). Information Warfare and the US Presidential Election. *Survival* 58 (5), 23-32. doi: 10.1080/00396338.2016.1231527

Inkster, N. (2015). *China's Cyber Power.* London: International Institute of Strategic Studies.

Jachtenfuchs, M. The monopoly of legitimate force: denationalization, or business as usual? In S. Leibfried and M. Zürn, *Transformation of the State?* (pp. 37-52). Cambridge: Cambridge University Press.

Janis, I. (1972). *Victims of Groupthink: A Psychological Study of Foreign-Policy Decisions and Fiascos.* Boston: Houghton Mifflin.

Johnston, A. I. (1999). Strategic Cultures Revisited: Reply to Colin Gray. *Review of International Studies*, 25 (3), 519-523. Retrieved from: https://www.jstor.org/stable/20097615? seq=1#page_scan_tab_contents

Johnston, A. I. (1998). *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History.* Princeton, NT: Princeton University Press.

Johnston, A. I. (1996). Cultural Realism and Strategy in Maoist China In P. J. Katzenstein, (Ed.). (1996). *The Culture of National Security Norms and Identity in World Politics* (pp. 216-256). New York: Columbia University Press.

Johnston, A. I. (1995). Thinking About Strartegic Culture. *International Security*, 19(4), 32-64. doi: 10.2307/2539119

Johnson, J. B., and Reynolds, H. T. (2005). *Political Science Research Methods (5th ed.).* Washington, D.C.: CQ Press.

Jun, J., LaFoy, S., & Sohn, E. (2015). *North Korea's Cyber Operations: Strategy and Responses* Washington D.C.: Center for Strategic and International Studies.

Junio, T. (2013). How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate *Journal of Strategic Studies* 36(1), 125-133. doi: 10.1080/01402390.2012.739561

Kahler, M. (1998). Rationality in International Relations *International Organization* 52 (4), 919-941. Retrieved by: https://www.jstor.org/stable/2601362

Kaldor, M. (2010). Inconclusive wars: is Clausewitz still relevant in these global times? *Global Policy*, 1 (3), 271-281. doi: 10.1111/j.1758-5899.2010.00041.x

Kaldor, M. (2005). Elaborating the 'New War' Thesis In J. Angstrom and I. Duyvesteyn, *Rethinking the Nature of War.* London: Frank Cass.

Kallender, P. and Hughes, C. W. (2017). Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace. *Journal of Strategic Studies,* 40 (1-2), 118-145.

Kamluk, V. (Ed.) (2017) *Lazarus Under the Hood.* Kaspersky Lab: Moscow, Russia.

Katagiri, N. (2015). Strategy and Grand Strategy for the Future of Asia. *Asian Survey,* 55(6), 1170-1192. doi: 10.1525/as.2015.55.6.1170

Katzenstein, P. J. (Ed.). (1996). *The Culture of National Security Norms and Identity in World Politics.* New York: Columbia University Press.

Karatzogianni, A. (2015). *Firebrand Waves of Digital Activism 1994-2014*. London: Palgrave, Macmillan.

Kao, M.M. (2011). *Strategic Culture of Small States: The Case of ASEAN* (unpublished doctoral thesis). Arizona State University.

Keck, Z. (2014, February). S. Korea Seeks Cyber Weapons to Target North Korea's Nukes. The Diplomat. Retrieved from http://thediplomat.com/2014/02/s-korea-seeks-cyber-weapons-to-target-north-koreas-nukes/

Kello, L. (2017). *The Virtual Weapon and International Order* London: Yale University Press.

Kello, L. (2013). The Meaning of the Cyber Revolution Perils to Theory and Statecraft. *International Security, 38*(2), 7-40. doi: 10.1162/ISEC_a_00138

Keohane, R. O. (1984). *After hegemony : cooperation and discord in the world political economy*. Princeton, N.J.: : Princeton University Press

Keohane, R. O. (1969). Lilliputians Dilemmas - Small States in International Politics *International Organization, 23*(2), 291-310. doi: 10.1017/S002081830003160X

Keohane, R. O., & Nye Jr., J. S. (2012). *Power and Indepedence* (4th ed.). Boston : Longman.

Keohane, R. O., & Nye, J. S. (1998). Power and interdependence in the information age. *Foreign Affairs, 77*(5), 81-94. doi: 10.2307/20049052

Kershaw, R. (2011)

Kernshaw, R. (2001) *Monarchy in South-East Asia: The Faces of Tradition in Transition.* London: Routledge.

Key. J. (2016, May 5). Speech to the Cyber Security Summit. Retrieved from: https://www.connectsmart.govt.nz/alertsnews/speech-to-cyber-security-summit/

Kibbe, J. (2012). Cuba, Angola, and the Soviet Union In S. E. L. Kristen P. Williams, Neal G. Jess (Eds.), *Beyond Great Powers and Hegemons: Why Secondary States Support, Follow or Challenge.* California: Stanford University Press.

Kier, E. (1995). Culture and Military Doctrine: France between the Wars *International Security*, 19 (4), 65-93. doi: 10.2307/2539120

Kim, S. (2015, November). South Korea enlists cyber warriors to battle Kim Jong-un's regime. Retrieved from http://www.independent.co.uk/news/world/asia/south-korea-enlists-cyber-warriors-to-battle-kim-jong-un-s-regime-a6753041.html

Kirkman, G.S., Cornelius. P. K., Sachs, J. D. and Schwab, K. (2002). The Global Information Technology Report 2001–2002. Oxford: Oxford University Press.

Kitteridge, R .(2013). *Review of Compliance at the Government Communications Security Bureau.* Wellington: Government Communications Security Bureau.

Klimburg, A. and Mirtl, P. (2012) *Cyberspace and Governance—A Primer* (Working Paper 65) Retrieved from: http://www.oiip.ac.at/publikationen/arbeitspapiere/publikationen-detail/article/92/cyberspace-and-governance- a-primer.html

Kline, R. R. (2001). Technological determinism. In N. J. Smelser and P. B. Baltes (Eds.), *International Encyclopedia of the Social & Behavioral Sciences* (pp. 15495–98). New York City: Elsevier.

Korns, S. W., & Kastenberg, J. E. (2009). Georgia's Cyber Left Hook. *Parameters*, 38(4), 60-76. Retrieved from: https://ssi.armywarcollege.edu/pubs/parameters/articles/08winter/korns.pdf

Knapp, K. J., & Boulton, W. R. (2006). Cyber-Warfare Threatens Corporations: Expansion Into Commercial Environments. *Information Systems Management, 23*(2), 76-87. doi: 10.1201/1078.10580530/45925.23.2.20060301/92675.8

Kramer, F. D., Starr, S. H., and Wentz, S. H. (Eds.) (2009). *Cyberpower and National Security*. Washington D.C.: Potomac Books, Inc.

Krause, K. (1992). Arms and the state : patterns of military production and trade. Cambridge , New York: Cambridge University Press.

Krepinevich, A. (2012). *Cyber Warfare: A "Nuclear Option"?* Washington D.C.: Center for Strategic and Budgetary Assessments

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem In F. D. Kramer, S. H. Starr, and L K. Wentz (Eds.), *Cyberpower and National Security* (pp. 24-42). Washington D.C.: Potomac Books, Inc.

Kurlantzick, J. (2007). Pax Asia-Pacifica? East Asian integration and its implications for the United States. *Washington Quarterly, 30*(3), 67-77. doi: 10.1162/wash.2007.30.3.67

Kvochko, E. (2013, 11 April). Five ways Technology can help the Economy *World Economic Forum*. Retrieved from: https://www.weforum.org/agenda/2013/04/five-ways-technology-can-help-the-economy/

Kydd, A. (2000). Trust, Reassurance, and Cooperation. *International Organization* 54 (2), 325-357.

Lakatos, I. (1970). Falsification and the Methodology of Scientific Research Programs In I. Lakatos and A. Musgrave (Eds.), *Criticism and the Growth of Knowledge* (pp. 131–132). Cambridge: Cambridge University Press.

Laksmana, E. (2017). (2017) Threats and Civil–Military Relations: Explaining Singapore's "trickle down" Military Innovation, *Defense & Security Analysis* 33 (4), 347-365.

Langø, H. (2013). *Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security*. Oslo, Norway: Norwegian Institute of International Affairs:

LaMontagne, P. (2016) *Operation Blockbuster: Unveiling the Long Tread of the Sony Attack*. Mclean, VA.: Novoletta.

Lantis, J. (Eds.) (2014). Strategic Cultures and Security Policies in the Asia-Pacific *Contemporary Security Policy* 35(2), 165-328. doi: 10.1080/13523260.2014.927676

Lantis, J. S., & Howlet, D. A. (2013). Strategic Culture In J. Baylis, J. J. Wirtz and C. S. Gray (Eds.), *Strategy in the Contemporary World* (4th ed.). Oxford: Oxford University Press.

Lantis, J. S., (2002). Strategic Culture and National Security Policy *International Studies Review* 4 (3), 87-113. doi: /10.1111/1521-9488.t01-1-00266

Larsen, E. (2005). *Analysing the Foreign Policy of Small States in the EU.* London: Palgrave MacMillan.

Lawrey, Roger Neil (2010). An Economist's Perspective on Economic Diversification in Brunei Darussalam. *CSPS Strategy and Policy Journal*, 1 (July), 13-28.

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats, *Journal of Information Technology & Politics* 10(1) 86-103. doi: 10.1080/19331681.2012.759059

Layne, C. (2006). *The Peace of Illusions: American Grand Strategy from 1940 to the Present.* Ithaca, N.Y.: Cornell University Press.

Layne, C. (2006a). Unipolar Illusion Revisited. *International Security, 31*(2), 7-41. doi: 10.1162/isec.2006.31.2.7

Leach, B. L. (2002). Interview Methods in Political Science *Politics and Political Science,* 35, 663-664. doi: 10.1017/S1049096502001117

Lee, H. l. (2014, November 24) Launch of Smart Nation Initiative, Speech at Smart Nation Launch. Retrieved from: http://www.pmo.gov.sg/newsroom/transcript-prime-minister-lee-hsien-loongs-speech-smart-nation-launch-24-november

Lee, K. Y. (1999, October 7). Speech at the Commemoration Conference of Confucius' 2550th Birthday and the 2nd Congress Of The International Confucius Association, Retrieved from: http://www.nas.gov.sg/archivesonline/speeches/view-html?filename=1999100706.htm

Leech, B. L. (2002). Interview Methods in Political Science *PS: Political Science and Politics* 35 (4), 663-664. doi: 10.1017/S1049096502001117

Lefebvre, S. (2003). The Difficulties and Dilemmas of International Intelligence Cooperation *International Journal of Intelligence and CounterIntelligence*, 16 (4), 527-542. doi: 10.1080/716100467

Legro, J. W. (1994). Military Culture and Inadvertent Escalation in World War II. *International Security* 18(4), 108-142. doi: 10.2307/2539179

Legro J. W. and Moravcsik, A. (1999) Is Anybody Still a Realist? *International Security,* 24 (2), pp. 5–55. doi: 10.1162/016228899560130

Lewis, J., & Timlin, K. (2011). *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*. Washington, D.C.: Center for Strategic and International Studies.

Lewis, J. A., & Neuneck, G. (2013). *The Cyber Index: International Security Trends and Realities*. Geneva, Switzerland: United Nations Institute for Disarmament Research.

Lew, J.A. (2018). Significant Cyber Incidents Since 2006. Washington, D.C.: Center for Strategic and International Studies.

Li, J.J. and Daugherty, L. (2015).*Training Cyber Warriors: What Can Be Learned from Defense Language Training?* Santa Monica, CA.: RAND Corporation.

Libicki, M. C. (2013). *Brandishing Cyberattack Capabilities*. Santa Monica, CA: RAND Corporation.

Libicki, M. C. (2012). Cyberspace Is Not a Warfighting Domain. *I/S: A Journal of Law and Policy for the Information*, 8(2), 325-340.

Libicki, M. (2011). The Strategic Uses of Ambiguity in Cyberspace. *Military and Stratgic Affair*s, 3(3), 3-10.

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica, California: RAND Corporation.

Libicki, M. C. (2007). *Conquest in Cyberspace National Security and Information Warfare*. New York: Cambridge University Press.

Liff, A. P. (2012). Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies, 35*(3), 401-428. doi: 10.1080/01402390.2012.663252

Lim, D. J., & Cooper, Z. (2015). Reassessing Hedging: The Logic of Alignment in East Asia, *Security Studies*, 24(4), 696-727. doi: 10.1080/09636412. 2015.1103130

Limnéll, J. (2016). The Cyber Arms Race is Accelerating – What are the Consequences? *Journal of Cyber Policy,* 1 (1), 50-60. doi: 10.1080/23738871. 2016.1158304

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies, 22*(3), 365-404. doi: 10.1080/09636412.2013.816122

Lindsay, J. R & Gartzke, E. (2018). *Coercion through Cyberspace: The Stability-Instability Paradox*. In Kelly Greenhill and Peter Krause. (Eds.), *The Power to Hurt: Coercion in the Modern World*. Oxford: Oxford University Press.

Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (Eds.). (2015). *China and Cybersecurity: Strategy, and Politics in the Digital Domain*. New York: Oxford University Press.

Lobell, S. E., Ripsman, N. M., & Taliaferro, J. W. (Eds.). (2009). *Neoclassical Realism, the State, and Foreign Policy*. Cambridge: Cambridge University Press.

Locke, R. M. and Thelen, K. (1998). Apples and Oranges Revisited: Contextualized Comparisons and the Study of Comparative Labor Politics. *Politics & Society* 23(3), 337-367.

Longhurst, K. (2004) *Germany and the Use of Force*. Manchester: Manchester University Press.

Loo, B. F. W. (2012) Goh Keng Swee and the Emergence of a Modern SAF In E. Chew and G.K. Chong (Eds.), *Goh Keng Swee: A Legacy of Public Service* (pp. 127-151). Singapore: World Scientific.

Loo, B. F. W. (Ed.). (2009). *Military Transformation and Strategy: Revolutions in Military Affairs and Small States*. London: Routledge.

Loo, B. F. W. (2005). Transforming the Strategic Landscape of Southeast Asia. *Contemporary Southeast Asia 27*(3), 388-405. doi:

Lord, K. M. (2006). National Intelligence in the Age of Transparency In L. Johnson (Ed.) *Strategic Intelligence* (pp. 181-200). Westport, CT: Praeger.

Lynch, M. (2002). Why Engage? China and the Logic of Communicative Engagement. *European Journal of International Relations, 8*(2), 187-230. doi: 10.1177/ 1354066102008002002

Lynn, W. (2011). Pentagon's Cyberstrategy, One Year Later. *Foreign Affairs* Retrived from: https://www.foreignaffairs.com/articles/2011-09-28/ pentagons-cyberstrategy-one-year-later

Lynn, W. (2010). Defending a New Domain The Pentagon's Cyberstrategy. *Foreign Affairs*, 89(5), 97-108. Retrieved from: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Lucas, G. (2017). *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare George Lucas.* Oxford: Oxford University Press.

Lynn, W. (2011, September ). The Pentagon's Cyberstrategy, One Year Later. *Foreign Affairs.* Retrived from https://www.foreignaffairs.com/ articles/2011-09-28/pentagons-cyberstrategy-one-year-later

Maass, M. (2009). The elusive definition of the small state. *International Politics,* 46(1), 65-83. doi: 10.1057/ip.2008.37

Mahnken, T. G. and Blumenthal, D. (2014). *Strategy in Asia.* California: Stanford University Press.

Mahnken, T. G. and Goldman, E. (2004) *The Information Revolution in Military Affairs in Asia.* London: Palgrave Macmillan.

Mahnken, T. G. (2012). *Competitive Strategies for the 21st Century.* California, U.S.: Stanford University Press.

Mahnken, T. G, (2008). *Technology and the American Way of War.* New York: Columbia University Press.

Mahoney, J. and Goertz, G. (2004). The Possibility Principle: Choosing Negative Cases in Comparative Research *American Political Science Review* 98(4), 653-669. doi: 10.1017/S0003055404041401

Mahoney, J. (2000). Path Dependence in Historical Sociology. *Theory and Society*, 29(4), 507-548. doi: 10.1023/A:1007113830879.

Majid, H. A. (2007). *Rebellion in Brunei: The 1962 Revolt, Imperialism, Confrontation and Oil.* London: I.B. Tauris.

Manjikian, M. M. (2010). From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly, 54*(2), 381-401. doi: 10.1111/j.1468-2478.2010.00592.x

Manson, G. P. (2011). Cyberwar: The United States and China Prepare for the Next Generation of Conflict. *Comparative Strategy*, 30(2), 121–133. doi: 10.1080/01495933.2011.561730

Matthews, R. and Yan, N.Z. (2007). Small Country 'Total Defence': A Case Study of Singapore 7 (3), 376-395. doi: 10.1080/14702430701559289

Maurer, T. (2018). *Cyber Mercenaries: The State, Hackers and Power.* Cambridge: Cambridge University Press.

Maurer, T. (2015). *Cybersecurity and Asia.* Washington, D.C.: New America.

Maurer, T. (2011). *Cyber Norm Emergence in the United Nations.* Cambridge, MA: Belfer Center for Science and International Affairs, Harvard University.

McCarthy, D. (2015). *Power, Information Technology, and International Relations Theory.* London: Palgrave Macmillan.

McChesney, R. W. (2014). *Digital Disconnect: How Capitalism is Turning the Internet Against Democracy*. New York The New Press.

McCraw, D. (2011). Change and Continuity in Strategic Culture: the Cases of Australia and New Zealand. *Australian Journal of International Affairs*, 65 (2), 167-184. doi: 10.1080/10357718.2011.550102

McGraw, D. (2008). New Zealand's Defence Policy: From Realism to Idealism?, *Defense & Security Analysis,* 24 (1), 19-32. doi: 10.1080/14751790801903194

McGuffin, C. & Mitchell, P. (2014). On domains: Cyber and the Practice of Warfare *International Journal*, 69(3) 394–412. doi: 10.1177/ 0020702014540618

McHugh, J., Allen, J., & Christie, A. (2000). Defending Yourself: The Role of Intrusion Detection Systems *IEEE Software*, 17(5), 42-51. doi: 10.1109/52.877859

McKirdy, E. and Lendon, B. (2017, August 23). US Navy 7th Fleet commander dismissed, Navy says. Retrieved from: https://edition.cnn.com/2017/ 08/22/politics/uss-mccain-7th-fleet-commander-dismissal/index.html

Mearsheimer, J.J. and Walt, S. (2013). Leaving Theory Behind: Why Simplistic Hypothesis Testing is Bad for IR, *European Journal of International Relations,* 19 (3), 427-57.

Mearsheimer, J. J. (2010). The Gathering Storm: China's Challenge to US Power in Asia. *Chinese Journal of International Politics, 3*(4), 381-396. doi: 10.1093/cjip/poq016

Mearshiermer, J. J. (2001). *The Tragedy of Great Power Politics*. New York: Norton & Company Inc.

Mearshiermer, J. J. (1995). The False Promise of International Institutions. *International Security*, 19 (3), 5-49. doi: 10.2307/2539078

Meilinger, P. S. (2010). The Mutable Nature of War. *Air & Space Power Journal* 24 (4), 24-30.

Mehdiyeva, N. (2011). *Power Games in the Caucasus: Azerbaijan's Foreign and Energy Policy Towards the West, Russia and the Middle East.* London: I.B.Tauris & Co Ltd.

Midgley, J., Arashi, R., Cloud, C., Moyer, J. M., & Strauss, B. (2016). *Asia-Pacific Defense Outlook 2016: Defense in Four Domains*. Tokyo, Japan: Deloitte Tohmatsu Consulting LLC.

Milner, H. (1991). The Assumption of Anarchy in International Relations Theory: A Critique. *Review of International Studies, 17*(1), 67-85. doi 10.1017/ S026021050011232X;

Miller, S. (2016). Cyber-attacks and 'Dirty Hands': Cyberwar, Cyber-crimes or Covert Political Action? In Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser (Eds.), *Binary Bullets: The Ethics of Cyberwarfare* (pp. 229-250) Oxford: Oxford University Press.

Minárik, T. (2016). ASEAN to Focus on Cybersecurity Capacity- and Confidence Building in 2017. Retrieved from: https://ccdcoe.org/asean-focus-cybersecurity-capacity-and-confidence-building-2017.html

Modi, C., Patel , D., Bhavesh, B., Patel, H., Patel , A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. *Journal of Network and Computer Applications*, 36(1), 42-57. doi: 10.1016/j.jnca.2012.05.003

Moravcsik, A. (1997). Taking Preferences Seriously: A Liberal Theory of International Politics *International Organization* (51) 4, 513-553. Retrieved from: http://www.jstor.org/ stable/2703498

Morozov, E. (2012). *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs.

Mulvenon, J. (2009). PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability In Roy Kamphausen, David Lai, and Andrew Scobell (Eds.), *Beyond the Strait: PLA Missions Other Than Taiwan* (pp. 253–285.). Carlisle, PA: Strategic Studies Institute, U.S. ArmyWar College Press.

Muller. G., Parr, G., Kubiak, L. and others (2016). *From Tech Sector to Digital Nation*. Auckland: New Zealand Technology Industry Association.

Müller, D. M. (2015). Sharia Law and the Politics of "Faith Control" in Brunei Darussalam Dynamics of Socio-Legal Change in a Southeast Asian Sultanate. *Internationales Asienforum,* 46 (3–4), 313–345.

Mumford, A. (2013). *Proxy War*. Oxford: Polity Press.

Nakashima, E. (2017, June 12) Russia has developed a cyberweapon that can disrupt power grids, according to new research. Retrieved from: https://www.washingtonpost.com/world/national-security/russia-has-developed-a-cyber-weapon-that-can-disrupt-power-grids-according-to-new-research/2017/06/11/b91b773e-4eed-11e7-91eb-9611861a988f_ story.html?utm_term= .fc27192c0910#comments

Naughton, J. (2016). The Evolution of the Internet: From Military Experiment to General Purpose Technology, *Journal of Cyber Policy,* 1 (1), 5-28. doi: 10.1080/23738871.2016.1157619

Narizny, K. (2017). On Systemic Paradigms and Domestic Politics: A Critique of the Newest Realism. *International Security*, 42 (2), 155-190.

Neumann, I. B. and Gstohl, S. (2006) "Introduction: Lilliputians in Gulliver's World?" In C. Ingebritsen, B. Neumann, S. Gstohl and J. Beyer (eds) *Small States in International Relations* (pp. 12–37) Seattle, WA: University of Washington Press.

New Zealand Defence Force (2012). *New Zealand Defence Doctrine (Third Edition)* Wellington: New Zealand Defence Force.

New Zealand Defence Force (2012). *New Zealand Defence Force: Future 35*. Wellington: New Zealand Defence Force.

New Zealand Government Communications Security Bureau (2015) *Annual Report.*Wellington: Government Communications Security Bureau.

New Zealand Government Communications Security Bureau (2014). *Annual Report*. Wellington: Government Communications Security Bureau.

New Zealand Government Communications Security Bureau. (2014a). *Project Cortex Business Case*. Wellington: Government Communications Security Bureau.

New Zealand National Cyber Policy Office. (2015a). *New Zealand's National Cyber Security Action Plan 2015*. Wellington, New Zealand: Department of Prime Minister and Cabinet.

New Zealand National Cyber Policy Office. (2015b). *New Zealand's National Cyber Security Strategy 2015*. Wellington, New Zealand: Department of Prime Minister and Cabinet.

New Zealand National Cyber Policy Office. (2015c). *National Plan to Address Cybercrime 2015*. Wellington, New Zealand: Department of Prime Minister and Cabinet.

New Zealand Ministry of Business, Innovation & Employment. (2015). *New Zealand Sectors Report Series: Information and Communications Technology*. Wellington: Ministry of Business, Innovation & Employment.

New Zealand Ministry of Business, Innovation & Employment. (2014). *New Zealand Sectors Report 2014*. Wellington: Ministry of Business, Innovation & Employment.

New Zealand Ministry of Business, Innovation & Employment (2017). *The Investor's Guide to the New Zealand Technology Sector*. Wellington: Ministry of Business, Innovation & Employment.

New Zealand Ministry of Defence. (2018). *Strategic Defence Policy Statement*. Wellington: Ministry of Defence.

New Zealand Ministry of Defence. (2016). *Defence White Paper 2016*. Wellington: Ministry of Defence.

New Zealand Ministry of Defence. (2014). *Defence Capability Plan*. Wellington: Ministry of Defence.

New Zealand Ministry of Foreign Affairs and Trade (2015). *Strategic Intentions 2015-2019*. Wellington: Ministry of Foreign Affairs and Trade.

New Zealand Treasury (2016). *New Zealand: Economic and Financial Overview 2016*. Wellington: The Treasury.

Ng. E. H. (2017, March 3). A Next Gen SAF to Combat New Threats, Speech by Minister for Defence Dr Ng Eng Hen at the Committee of Supply. Retrieved from: https://www.mindef.gov.sg/imindef/press_room/ details.html?name= 03mar17_ speech1&date=2017-03-03#. WdNQb1tSyUk

Nissenbaum, H. (2005). Where Computer Security Meets National Security *Ethics and Information Technology* 7 (2), 61-73. doi: 10.1007/s10676-005-4582-3

Nocetti, J. (2015). Contest and Conquest: Russia and Global Internet Governance *International Affairs* 91 (1), 111-130. doi: 10.1111/1468-2346.12189

North Atlantic Treaty Organisation. (2018). Cyber Security Strategy Documents. Retrieved from 16 July 2018, from: https://ccdcoe.org/cyber-security-strategy-documents.html

North Atlantic Treaty Organisation. (2016, 8 July). Cyber Defence Pledge. Retrieved 16 July 2018, from: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

North Atlantic Treaty Organization. (2014, September 5).Wales Summit Declaration. Retrieved from: http://www.nato.int/cps/ic/natohq/official_texts_112964.htm

Nye, J. (2017). Deterrence and Dissuasion in Cyberspace. *International Security,* (41) 3, 44–71. doi:10.1162/ISEC_a_00266

Nye, J. S. (2010). *Cyber Power.* Cambridge, MA: Belfer Center for Science and International Affairs, Harvard University.

Nye, J. S. (2011). Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly, 5*(4), 18-38. Retrived from: https://dash.harvard.edu/bitstream/handle/1/8052146/Nye-NuclearLessons.pdf

Nye, J. S. (2007). *Understanding International Conflicts: An Introduction to Theory and History* (6th ed.). New York: Pearson.

Nye Jr., J. S., & Owens, W. S. (1996). America's Information Edge. *Foreign Affairs, 75*(3), 20-36. Retrieved from: https://www.foreignaffairs.com/issues/1996/75/2

Obama, B. (2011). *International Strategy for Cyberspace.* Washington, D.C.: The White House.

Obama, B. (2012). Taking the Cyberattack Threat Seriously *Wall Street Journal* Retrieved by: https://www.wsj.com/articles/SB1000087239639 0444330904577535492693044650

Observatory of Economic Complexity (2015). "New Zealand" Retrieved from: http://atlas.media.mit.edu/en/profile/country/nzl/

O'Connell, M. E. (2012). Cyber Security without Cyber War *Journal of Conflict & Security Law* 17(2), 187–209. doi: 10.1093/jcsl/krs017

Oettinger, G.H. (2015, June). Speech Cybersecurity Strategy. Retrieved from https://ec.europa.eu/commission/2014-2019/oettinger/announcements/speech-cybersecurity-strategy-28-may-2015_en

O'Hanlon, M. (2000). *Technological Change and the Future of Warfare.* Washington D.C.: Brookings Institution Press.

O'Neil, A. (2017). Australia and the 'Five Eyes' intelligence network: the perils of an asymmetric alliance. *Australian Journal of International Affairs* 71(5), 529-543.

Ólafsson, B. G. (1998). *Small States in the Global System: Analysis and Illustration from* the *Case of Iceland.* Aldershot, UK: Ashgate.

Oishi, M. (2015). Brunei's Foreign Relations: Maintaining and Developing Its Identity in a Rapidly Changing World In O. K. Gin (Eds.), *Brunei – History, Islam, Society and Contemporary Issues* (pp. 62-78). London: Routledge.

Ortis, C., & Evans, P. (2003). The Internet and Asia-Pacific security: old conflicts and new behaviour. *Pacific Review, 16*(4), 549-572. doi: 10.1080/0951274032000132254

Owen, T. (2015). *Disruptive Power: The Crisis of the State in the Digital Age* Oxford: Oxford University Press.

Panetta, L. E. (2012, October) Remarks on Cybersecurity to the Business Executives for National Security, New York City, 11 October 2012, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136

Panke, D. (2017). Studying small states in International Security Affairs: A Quantitative Analysis, *Cambridge Review of International Affairs*, 30(2-3), 235-255. doi: 10.1080/09557571.2017.1313194

Parameswaran, P. (2017). China Navy Fleet Makes Brunei Voyage. *The Diplomat* Retrieved from: https://thediplomat.com/2017/09/china-navy-fleet-makes- brunei-voyage/

Parameswaran, P. (2016) ASEAN Defense Chiefs Agree to New Cybersecurity Group *The Diplomat* Retrieved from: https://thediplomat.com/2016/ 06/asean-defense-chiefs- agree-to-new-cybersecurity-group/

Pastor, R. (1993). The United States and Central America: Interlocking Debates In P. Evans, H. K. Jacobson & R. D. Putnam (Eds.), *Double-Edged Diplomacy: International Bargaining and Domestic Politics*. Berkeley, California: University of California Press.

Patman, R. and Southgate, L. (2016). National Security and Surveillance: The Public Impact of the GCSB Amendment Bill and the Snowden Revelations in New Zealand *Intelligence and National Security* 31 (6), 871-887. doi: 10.1080/02684527.2015.1095968

Patton, M. Q. (2002). *Qualitative Research & Evaluation Methods* (3rd ed.*)*. Thousand Oaks, CA: Sage Publications.

Pape, R. (1996). *Bombing to Win: Air Power and Coercion in War*. Ithica, New York: Cornell University Press.

Pape, R. A. (2005). Soft balancing against the United States. *International Security, 30*(1), 7-45. doi: 10.1162/0162288054894607

Peou, S. (2002). Constructivism in Security Studies on Pacific Asia: Assessing Its Strengths and Weaknesses. *Pacific Focus*, 17(2), 177-211. doi: 10.1111/j.1976-5118.2002.tb00273.x

Phneah, E. (2013, July 1). Singapore Creates Operations Hub to Beef Up Cyberdefense *ZDnet* Retrieved from: http://www.zdnet.com/ article/singapore-creates-operations-hub-to-beef-up-cyberdefense/

Porter, P. (2015). *The Global Village Myth* London: Hurst & Company.

Porter, P. (2013). *Sharing Power? Prospects for A U.S. Concert-Balance Strategy*. Carlisle, PA: U.S. Army War College Press.

Porche, I. (2010, December 9). Stuxnet is the World's Problem. *Bulletin of the Atomic Scientists*. Retrieved from: https://thebulletin.org/stuxnet-worlds-problem

Poznansky, M. and Perkosky, E. (2018). Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution *Social Science Research Network* Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836087

Praprotnik, G., et. al. (2012). A Slovenian Perspective on Cyber Warfare. In D. Ventre (Ed.), *Cyber Conflict Competing National Perspectives*. London, UK: ISTE, Ltd.

Putnam, R. (1988). Diplomacy and Domestic Politics: The Logic of Two-Level Games *International Organization, 42*(3), 427-460. doi: 10.1017/ S0020818300027697

Ragnarsson, J. K. & Bailes, A. J. K. (2011). Iceland and Cyber-Threats: Is it More than Fear of Fear? *Icelandic Review of Politics and Administration* 7(1), 187-204. doi: 10.13177/irpa.a.2011.7.1.10

Rahman, C.  and Tsamenyi, M. (2010). A Strategic Perspective on Security and Naval Issues in the South China Sea. *Ocean Development & International Law* 41 (4),  315-333. doi: 10.1080/00908320.2010.499277

Rajaratnam, S. (1972). *Singapore: A Global City*. Singapore: National Achieves of Singapore. Retrieved from: http://www.nas.gov.sg/archivesonline/data/ pdfdoc/PressR19720206a.pdf

Rapley, T. (2008). *Doing Conversation, Discourse and Document Analysis* London: Sage Publications.

Raska, M. (2016). *Military Innovation in Small States: Creating Reverse Asymmetry*. New York: Routledge.

Raska, M. (2015). *Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy*. Singapore: S. Rajaratnam School of International Studies.

Raska, M. (2011). *Searching For New Security Paradigms: Israel and South Korea's Defense Transformation (1990-2011)* (unpublished doctoral thesis). National University of Singapore.

Raska, M. (2011a). The "Five Waves" of RMA Theory. *Pointer: Journal of the Singapore Armed Forces* 36 (3-4), 1-12. doi: https://www.mindef.gov.sg/ oms/imindef/ publications/pointer/index.html

Rattray, G. (2009). An Environmental Approach to Understanding Cyberpower. In F. D. Kramer, S. H. Starr, and L K. Wentz (Eds.), *Cyberpower and National Security* (pp. 253-274). Washington D.C.: Potomac Books, Inc.

Rattray, G. (2001). *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press.

Raudzens, G. ( 1990). War-Winning Weapons: The Measurement of Technological Determinism in Military History *Journal of Military History, 54*(4), 403-434. doi: 10.2307/1986064

Reardon, R., & Choucri, N. (2012). *The Role of Cyberspace in International Relations: A View of the Literature*. Paper presented at the International Studies Association Annual Convention San Diego, CA.

Reiber, J. and Sukumar, A. M. (2017). *Asian Cybersecurity Futures: Opportunity and Risk in the Digital World*. Center For Long-Term Cybersecurity: U.C. Berkley.

Reiter, E., & Gärtner, H. (Eds.). (2001). Small States and Alliances. Heidelberg: Physica-Verlag Heidelberg.

Reveron, D. (Ed.). (2012). *Cyberspace and National Security: Threats, Opportunities, and  Power in a Virtual World* Washington D.C.: Georgetown University Press.

Resende-Santos, J. (2007). *Neorealism, States, and the Modern Mass Army*. Cambridge Cambridge University Press.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies,* 35 (1), 5-

32.

Rid, T. (2013). *Cyberwar will Not Take Place*. London: Hurst & Co. Ltd.

Rid, T. & Buchanan, B. (2015). Attributing Cyber Attacks *Journal of Strategic Studies*. 38 (1-2), 4-37.

Rid, T. & McBurney, P. (2012). Cyber-Weapons. *RUSI Journal* 157(1), 6-13.

Rinehart, I. E. and Elias, B. (2015). *China's Air Defense Identification Zone (ADIZ)*. Washington D.C.: Congression Research Service.

Ripsman, N. M., & Taliaferro, J. W., and Lobell, S. E. (Eds.). (2016). *Neoclassical Realist Theory of International Politics*. Oxford: Oxford University Press.

Ritchie, J., and Lewis, J. (2003). *Qualitative research practice: A guide for social science students and researcher*s. London: Sage Publications.

Roberts C. B. and Cook, M. (2016). Brunei Darussalam: Challenging Stability In M. Cook and D. Singh (Eds.), *Southeast Asian Affairs* (pp. 95-105). Singapore: Institute of Southeast Asian Studies.

Roberts. C. (2014). Brunei in 2013 Paradoxes in Image and Performance? In D. Singh (Eds.), *Southeast Asian Affairs* (pp. 83-95). Singapore: Institute of Southeast Asian Studies.

Rogers, D. (2015). Extraditing Kim Dotcom: a case for reforming New Zealand's intelligence community?, *Kotuitui: New Zealand Journal of Social Sciences Online*, 10 (1), 46-57. doi: 10.1080/1177083X.2014.992791

Rosato, S. (2015). The Inscrutable Intentions of Great Powers. *International Security* 39(3), 48-88. doi: org/10.1162/ISEC_a_00190

Rose, G. (1998). Neoclassical realism and theories of foreign policy. *World Politics, 51*(1), 144-172. doi: 10.1017/S0043887100007814

Rosenau, J. (1980). *The Scientific Study of Foreign Policy* London: Nichols Publishing Company.

Rosenberg, N. (1994). *Exploring the Black Box Technology, Economics, and History*. Cambridge: Cambridge University Press.

Rosenzweig, P. (2013). *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World*. Santa Barbara, CA Praeger Publishers Inc.

Rosenau, J. (1980). *The Scientific Study of Foreign Policy*. New York Nichols Pub. Co.

Ross, R. (2006). Balance of Power Politics and the Rise of China: Accommodation and Balancing in East Asia. *Security Studies*, 15(3), 355-395. doi: 10.1080/09636410601028206

Roy, D. (2005). Southeast Asia and China: Balancing or Bandwagoning? *Contemporary Southeast Asia* 27 (2), 305–322. doi: 10.1017/ S1598240800002794

Roy, D. (1994). Hegemony on the Horizon - The China Threat to East-Asian Security *International Security, 19*(1), 149-168. doi: 10.2307/2539151

Rudner, M. (2013). Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. *International Journal of Intelligence and CounterIntelligence, 26*(3), 453-481. doi: 10.1080/08850607.2013.780552

Russell, A. (2017). *Strategic A2/D2 in Cyberspace*. Cambridge: Cambridge University Press.

Russell, A. (2015). *Strategic Anti-Access/Area Denial in Cyberspace* In M.Maybaum, A.-M.Osula, L.Lindström (Eds.), *7th International Conference on Cyber Conflict: Architectures in Cyberspace* (pp. 153-168). Tallin, Estonia: NATO CCD COE.

Russell, A. (2014). *Cyber Blockades.* Washington D.C.: Georgetown University Press.

Rustici, R. (2011). Cyberweapons: Leveling the International Playing Field. *Parameters,* 41(3), 32-42. Retrieved from: http://ssi.armywarcollege.edu/pubs/parameters/Articles/2011autumn/Rustici.pdf

Sachs, J. (2000). *Readiness for the Networked World: A Guide for Developing Countries.* Cambridge, MA: Center for International Development, Harvard University.

Samaan, J. (2010). Cyber Command, *RUSI Journal*, 155 (6), 16-21. doi: 10.1080/03071847. 2010.542664

Saunders, P. C. and Bowie, J.G. (2016). US–China Military Relations: Competition and Cooperation, *Journal of Strategic Studies*, 39(5-6), 662-684. doi: 10.1080/01402390.2016.1221818

Schaake, M. and Vermeulen, M. (2016). Towards a Values Based European Foreign Policy to Cybersecurity, *Journal of Cyber Policy* 1 (1) 75-84.

Schelling, T. (2008). *Arms and Influence.* New Haven, CT: Yale University Press (Original work published in 1966).

Schelling, T. (1981). *The Strategy of Conflict.* Cambridge, MA: Harvard University Press (Original work published in 1960).

Schia, N. N. (2018) The Cyber Frontier and Digital Pitfalls in the Global South, *Third World Quarterly* 39(5), 821-837. doi: 10.1080/01436597.2017.1408403

Schneier, B. (2010, 7 October). The Story Behind The Stuxnet Virus. *Forbes.* Retrieved from: https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology- security-stuxnet-worm.html#185b833051e8

Schroeder, P. (1994). Historical Reality vs. Neo-Realist Theory. *International Security, 19*(1), 108-148. Retreived from: https://www.jstor.org/stable/pdf/2539150.pdf?seq=1#page_scan_tab_contents

Schweller, R. L. (2006). *Unanswered Threats: Political Constraints on the Balance of Power.* Princeton, N.J.: Princeton University Press.

Schweller, R. L. (2003). The Progressiveness of Neoclassical Realism. In C. Elman & M. Elman (Eds.), *Progress in International Relations Theory* (pp. 311-348). Cambridge, MA.: MIT Press.

Schweller, R. L. (1993). Tripolarity and the Second World War. *International Studies Quarterly*, 37(1), 73-103. doi: 10.2307/2600832

Scott, D. (2012). Conflict Irresolution in the South China Sea. *Asian Survey* 52 (6), 1019-1042.

Scott, John (1990) *A Matter of Record.* Cambridge: Policy Press.

Segal, A. (2017). Cyber Operations Tracker. *Council of Foreign Relations.* Retrieved from: https://www.cfr.org/interactive/cyber-operations

Segal, A. (2017a, June 29). The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What? Retrieved from:

https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what

Segal, A. (2017b, 17 November). An Update on U.S.-China Cybersecurity Relations. *Council of Foreign Relations,* Retrieved from: https://www.cfr.org/blog/update-us-china-cybersecurity-relations

Sharp, T. (2017). Theorizing cyber coercion: The 2014 North Korean operation against Sony *Journal of Strategic Studies* 40 (7), 898-926. doi: 10.1080/01402390. 2017.1307741

Shambaugh, D. (1996). Containment or engagement of China? Calculating Beijing's Responses. *International Security, 21*(2), 180-209. doi: 10.2307/2539074

Sheldon, J. B. (2015). Rise of Cyber Power. In J. Baylis, J. J. Wirtz & C. S. Gray (Eds.), *Strategy in a Contemporary World* (4th ed.): Oxford University Press.

Sheldon, J. B. (2011). Deciphering Cyberpower: Strategic Purpose in Peace. *Strategic Studies Quarterly, 5*(2), 95-112. Retrieved by: http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-05_Issue-2/Sheldon.pdf

Shlapentokh, D. (2012). *The Role of Small States In The Post-Cold War Era: The Case of Belarus.* Carlisle Barracks, Pennsylvania: Strategic Studies Institute, U.S. Army War College.

Shulsky, A. N. and Schmitt, G. (2002). Silent Warfare: Understanding the World of Intelligence. Washington D.C.: Potomac Books, Inc.

Singh, J. P. (2013). Information Technologies, Meta-power, and Transformations in Global Politics *International Studies Review* 15 (1), 5-29.

Singapore Cyber Security Agency. (2016) *Singapore's Cybersecurity Strategy* Singapore: Cyber Security Agency.

Singapore Cyber Security Agency. (2016a) *Singapore Cyber Landscape.* Singapore: Cyber Security Agency.

Singapore Infocom Development Authority (2014). "Factsheet: Smart National Platform" Retrieved from: https://www.imda.gov.sg/~/media/imda/files/inner/about%20us/newsroom/media%20releases/2014/0617_smartnation/annexa_sn.pdf?la=en

Singapore Ministry of Defence (2017, March 3). Fact Sheet: Next Gen SAF's New Cyber Command to Combat Growing Cyber Threat. Retreived from: https://www.mindef.gov.sg/imindef/press_room/details.html?name=03mar17_fs2&date=2017-03-03#.WdN8DVtSyUk

Singapore Ministry of Defence (2015, December 8). Joint Statement by US Secretary of Defense Ashton Carter and Singapore Minister for Defence Dr Ng Eng Hen. Retreived from: https://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2015/08dec15_speech.html#.WdN9altSyUk

Singapore Ministry of Defence. (2013, January 10). "Total Defence" Retrieved from https://www.mindef.gov.sg/imindef/key_topics/total_defence.html

Singapore Ministry of Defence. (2005, September 16) Factsheet Information about IKC2 and Highlights of the Exhibition. Retreived from: https://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2005/sep/16sep05_nr/05sep05_fs.html

Singapore Ministry of Home Affairs (2016). National Cybercrime Action Plan. Singapore: Ministry of Home Affairs.

Singapore Prime Minister's Office. (2017, August 17). National Cybersecurity R&D Programme, Retrieved from: https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme

Singer, J. D. (1961). The Levels-of-Analysis Problem in International Relations. *World Politics, 14*(1), 77-92.

Singer, P., & Friedman, A. (2014). *Cybersecurity and Cyberwar*. Oxford: Oxford University Press.

Slayton, R. (2017) What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment *International Security* 43 (3), 72-109. doi: 10.1162/ISEC_a_00267

Sloan, E. (2012). *Modern Military Strategy: An Introduction*. London: Routledge.

Smeets, M. (2017). A Matter of Time: On the Transitory Nature of Cyberweapons *Journal of Strategic Studies,* 1-28. doi: 10.1080/01402390.2017.1288107

Smith, S. Hadfield, A. and Dunne, T. (Eds.) (2016). *Foreign Policy Theories, Actors and Cases.* Oxford: Oxford University Press.

Snyder, J. (1977). *The Soviet Strategic Culture: Implications for Limited Nuclear Operations*. Santa Monica: RAND Corporation.

Solomon, R. (2017). Electronic protests: hacktivism as a form of protest in Uganda *Computer Law & Security Review* 33 (5), 718–728.

Stapleton-Gray, R., & Woodcock, B. (2011). National Internet Defense—Small States on the Skirmish Line. *ACM Queue*, 9(1), 30-37. doi: 10.1145/1897852.1897869

Stavridis, J. (2017). *Sea Power: The History and Geopolitics of the World's Oceans*. New York: Penguin Random House.

Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P.,

Schöller, M.& Smith, P. (2010). Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines *Computer Networks* 54, 1245–1265.

Stevens, T. (2012). A Cyberwar of Ideas? Deterrence and Norms in Cyberspace, *Contemporary Security Policy* 33(1), 148-170. doi: 10.1080/13523260.2012.659597

Stewart, M. (2015, July 15). Spy conference shrouded in secrecy despite calls for transparency. *Stuff.* Retrieved from https://www.stuff.co.nz/national/politics/70254927/spy-conference-shrouded-in-secrecy-despite-calls-for-transparency

Sterbenz*,* J.P.G., Hutchiso, D., Çetinkaya E. K., Jabbar, A., Rohrera, J. P., Schöllerc, M. Smith, P. (2010). Resilience and Survivability in communication networks: Strategies, Principles, and survey of Disciplines. *Computer Networks,* 54 (8), 1245–1265. doi: 10.1016/j.comnet.2010.03.005

Stockholm International Peace Research Institute (2016). Military Expenditure Database. Retrieved from: https://www.sipri.org/databases/milex

Stokes, M. A. (2015). The Chinese People's Liberation Army Computer Network Operations Infrastructure In J. R. Lindsay, T. M. Cheung, and D. Reveron (Eds.), *China and Cybersecurity* (pp. 142-177) Oxford: Oxford University Press.

Stone, J. (2013). Cyber War Will Take Place! *Journal of Strategic Studies,* 36(1), 101-108. doi: 10.1080/01402390.2012.730485

Stoll, C. (2014). Cuckoo's Egg: Stalking the Wiley Hacker In Jason Healey (Ed.). *A Fierce Domain: Conflict in Cyberspace 1986 to 2012* (pp. 89-106). Virginia: Cyber Conflict Studies Association.

Swaine, M. D., Eberstadt, N. Fravel, M. T. Herberg, M. Keidel, A., Revere, E. J. R., Romberg, A. D…Wong, A. (2015). *Conflict and Cooperation in the Asia-Pacific Region: A Strategic Net Assessment.* Washington, D. C.: Carnegie Endowment for International Peace.

Swiss Federal Department of Defence (2012). *National strategy for Switzerland's protection against cyber risks.* Switzerland: Federal Department of Defence. Retrieved from: https://www.isb.admin.ch/isb/en/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html

Taiwan Ministry of Defence (2015). *National Defense Report 2015.* Taipei: Ministry of National Defense. Retrieved by: http://www.mnd.gov.tw/

Tan, A. T. H. (2014). *Arms Race in Asia: Trends, Causes and Implications* London: Routledge.

Tan, S. S. (2012). Faced with the Dragon: Perils and Prospects in Singapore's Ambivalent Relationship with China. *The Chinese Journal of International Politics* 5 (3), 245–265, doi. 10.1093/cjip/pos012

Tan, A. T. H. (Ed.) (2010). *The Global Arms Trade: A Handbook.* London: Routledge.

Tan, A. T. H. (2011). East Asia's Military Transformation: The Revolution in Military Affairs and its Problems, *Security Challenges,* 7 (3), 93-116.

Tan, A. T.H. (2003). Force Modernization in Southeast Asia *IDSS Working Paper Series* (Vol. 59). Singapore.

Tan, A. T. H. (1999). Singapore's Defence: Capabilities, Trends and Implications *Contemporary Southeast Asia* 21(3), 451-474.

Thayer, C. A. (2010). US Rapprochement with Laos and Cambodia. *Contemporary SoutheastAsia, 32*(3), 442-459. Retrieved from: http://www.jstor.org/stable/25798872

Thomas, N. (2009). Cyber Security in East Asia: Governing Anarchy. *Asian Security, 5*(1), 3-23. doi: 10.1080/14799850802611446

Talib, N.S. (2013). Brunei Darussalam: Royal Absolutism and the Modern State *Kyoto Review of Southeast Asia March* (Issue 13), pp. 1-8.

Talib, N.S. (2002). A Resilient Monarchy: The Sultanate of Brunei and Regime

Legitimacy In An Era of Democratic Nation-States *New Zealand Journal of Asian Studies* 4 (2), 134-147. Retrieved from: https://kyotoreview.org/wp-content/uploads/Naimah-English.pdf

Tan, A.T.H. (2014). *The Arms Race in Asia: Trends, Causes and Implications*. London: Routledge.

Tan, A.T.H. (2011). *East Asia's Military Transformation: The Revolution in Military Affairs and its Problems Security Challenges* 7(3), 71-94.

Tellis, A. J., Szalwinski, A. and Wills, M. (2016). *Understanding Strategic Cultures in the Asia-Pacific*. Washington D. C: The National Bureau of Asian Research.

Tehan, D. (2017, October 11). *New Cyber Security Centre in Melbourne to boost National Security*. Retrieved from: https://ministers.pmc.gov.au/tehan/2017/new-cyber-security-centre-melbourne-boost-national-security

Tiirmaa-Klaar, H., Gassen, J., Gerhards-Padilla, E., Martini, P. (2013). *Botnets*. Heidelberg: Springer.

Tisdell, C. (1998). Brunei's Quest for Sustainable Development: Diversification and other Strategies. *Journal of the Asia Pacific Economy* 3(3), 388-409. doi: 10.1080/13547869808724659

Tow, W.T. (1999). Strategic Cultures in Comparative Perspective In Ken Booth & Russell Trood (Eds.), *Strategic Cultures in the Asia-Pacific Region*. London: Palgrave Macmillan.

Tow, W.T. (2013). *Bilateralism, Multilateralism and Asia-Pacific Security*. London: Routledge.

UK Cabinet Office (2016). *National Cyber Security Strategy 2016-2021*. London: Cabinet Office.

U.S.–China Economic and Security Review Commission (2012). *2012 Report to Congress*. Washington D.C.: U.S. Government Printing Office.

U.S. Department of Defense (2010). *Joint Terminology for Cyberspace Operations*. Washington. D.C.: Department of Defense.

U.S. Department of Defense. (1999) . *DoD Dictiobnary of Military and Associated Terms (March 23, 1994 as amended through February 10, 1999)*. Washington, D.C.: Department of Defense.

U.S. Department of State (2017, September 13). U.S. Relations with Brunei. Retrieved from: https://www.state.gov/r/pa/ei/bgn/2700.htm

U.S. Office of the Director of National Intelligence (2017). *Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution*. Washington D.C.: Office of the Director of National Intelligence.

United Nations (2017). *World Population Prospects: The 2017 Revision*. New York: United Nations Population Division, Retrieved from: https://esa.un.org/unpd/wpp/

United Nations General Assembly (2013). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98. Retrieved from: http://www.un.org/ga/search/view_doc.asp?symbol= A/68/98

Valeriano, B., & Maness, R. (2016). Cyber Spillover: The Transition from Cyber Incident to Conventional Foreign Policy Dispute (pp. 45-64) In K. Friis and J. Ringsmose (Eds.), *Conflict in Cyberspace: Theoretical, Strategic and Legal Perspectives*. New York: Routledge.

Valeriano, B., & Maness, R. (2015). *Cyber War versus Cyber Realities: Cyber Conflict in the International System* Oxford: Oxford University Press.

Valeriano, B., & Maness, R. (2015a). *Russia's Coercive Diplomacy Energy, Cyber, and Maritime Policy as New Sources of Power.* London: Palgrave Macmillan.

Valeriano, B., & Maness, R. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research, 51*(3), 347-360. doi: 10.1177/0022343313518940

Valeriano, B. and Vasquez, J. A. (2010). Classification of Interstate Wars. *The Journal of Politics*, 72 (2), 1–18. doi: 10.1017/S0022381609990740

Valeriano, B., Maness, R. & Jensen, B. (2018). *International Relations Theory and Cyber Security* In C. Brown and R. Eckersley (Eds.), *The Oxford Handbook of International Political Theory* Oxford: Oxford University Press.

Valeriano, B., Maness, R. & Jensen, B. (2018a). *Cyber Strategy: The Evolving Character of Power and Coercion* Oxford: Oxford University Press.

Valeriano, B., Maness, R. & Jensen, B. (2017, July 13). Cyberwarfare has taken a new turn. Yes, it's time to worry. *Washington Post.* Retrieved from: https://www.washingtonpost.com/ news/monkey-cage/wp/2017/ 07/13/cyber-warfare-has-taken-a-new-turn-yes-its-time- to-worry/ ?utm_term=.a0c1b3f83219

Valeriano, B. and Vasquez. J. A. (2010). Identifying and Classifying Complex Interstate Wars 54 (2), 561-582. doi: 10.1111/j.1468-2478.2010.00599.x

Van Tol, J., Gunzinger, M., Krepinevich, A. F., and Thomas, J. (2010). *AirSea Battle: A Point-of-Departure: Operational Concept.* Washington D.C.: Center for Strategic and Budgetary Assessments.

Van Evera, S. (1998). Offense, Defense, and Causes of War. *International Security* 22 (4), 5-43.

Van Puyvelde, D. and Brantly, A. (2017). *US National Cybersecurity: International Politics, Concepts and Organization*. New York: Routledge.

Vellut. J. (1967). Smaller States and the Problem of War and Peace: Some Consequences of the Emergence of Smaller States in Africa *Journal of Peace Research* 4 (3), 252-269. doi: 10.1177/002234336700400303

Vennesson, P. (2017). Is Strategic Studies Narrow? Critical security and the Misunderstood Scope of Strategy. *Journal of Strategic Studies* 40 (3), 358-391. doi: 10.1080/01402390.2017.1288108

Vital, D. (1967). *The Inequality of States: A Study of The Small Power in International Relations.* Oxford: Clarendon Press.

Walsh, E. (2011). Brunei Darussalam's National Security Strategy. *ETH Zürich* Retrieved from: http://www.css.ethz.ch/en/services/digitallibrary/ articles/article.html/133571/pdf.

Walsh, P. and Miller, S. (2016). Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden. *Intelligence and National Security* 31 (3), 345-368. doi: 10.1080/02684527.2014.998436

Waltz, K .(2010). *Theory of International Politics* Illinios, U.S.: Waveland Press. (Original work published in 1979).

Waltz, K. (2000) Structuralism After the Cold War *International Security* 25 (1), 5-44. doi: 10.1162/016228800560372

Walt, S. M., & Mearsheimer, J. J. (2013). Leaving theory behind: Why simplistic hypothesis testing is bad for International Relations. *European Journal of International Relations, 19*(3), 427-457. doi: 10.1177/1354066113494320

Walt, S. M. (1985). Alliance of Formation and the Balance of World Order *International Security, 9*(4), 3-43. doi: 10.2307/2538540

Warden, J. A. (1992). Employing Air Power in the Twenty-first Century In R.H. Shultz, Jr. & R. L. Pfaltzgraff, Jr. (Eds.), *The Future of Airpower in the Aftermath of the Gulf War*. Maxwell AFB, AL: Air University Press, 1992.

Whaley, B. (1982). Toward a general theory of deception. *Journal of Strategic Studies* 5(1), 178-192. doi: 10.1080/01402398208437106

Wesley, M. (2009). 'Asia-Pacific institutions. In W. T. Tow (Ed.), *Security Politics in the Asia-Pacific: A Regional-Global Nexus?* (pp. 49-66). Cambridge, UK Cambridge University Press.

Weatherbee, D. E. (2014). *International relations in Southeast Asia: the struggle for autonomy*. Lanham, Maryland: Rowman & Littlefield.

Weber , A. M. (2003). The Council of Europe's Convention on Cybercrime *Berkley Technology* Law Journal 18(1), 425-446. Retrieved from: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1416&context=btlj

Weisberg, H. (2007). The Methodological Strengths and Weaknesses of Survey Research In W. Donsbach and M. W. Traugott (Eds.), *The Sage Handbook of Public Opinion Research* (pp. 223-231). London: Sage Publications.

Weller, G. R. (2001).The Internal Modernization of Western Intelligence Agencies, *International Journal of Intelligence and CounterIntelligence*, 14 (3), 299-322. doi: 10.1080/08850600152386828

Wendt, A. (1992). Anarchy is What States Make of It: the Social Construction of Power Politics *International Organization* 46 (2), 391-425. doi: 10.1017/ S0020818300027764

Wescott, N. (2008). *Digital Diplomacy: The Impact of the Internet on International Relations.* Oxford: Oxford Internet Institute.

Wicherski, G., Alperovitch, D., Contos, B. (2011). *Ten Days of Rain: Expert Analysis of Distributed Denial-of-Service Attacks Targeting South Korea* Santa Clara, CA.: McAfee.

Wiegand, K. E. (2011). Militarized territorial disputes: states' attempts to transfer reputation for resolve J*ournal of Peace Research* 48 (1), 101-113. doi: 10.1177/0022343310389414

Williams, G. (2017, May 6). 'Cyber doesn't respect borders': GCHQ's security chief on the dangers facing the UK. *Wired* Retrieved by: http://www.wired.co.uk/article/ cyber-threats-uk-ciaran-martin

Williams, K. P. (2012). Romania's Resistance to the USSR In S. E. L. Kristen P. Williams, Neal G. Jess (Eds.), *Beyond Great Powers and Hegemons: Why Secondary States Support, Follow or Challenge*. California: Stanford University Press.

Williams, B. T. (2014). The Joint Force Commander's Guide to Cyberspace Operations*Joint Forces Quarterly* 73 (1), 12-19. Retrived from: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf?ver=2014-04-01-122156-563

Williams, K. P. (2012). Romania's Resistance to the USSR In K. P. Williams, S. E. Lobell, and N. G. Jess (Eds.), *Beyond Great Powers and Hegemons: Why Secondary States Support, Follow or Challenge*. California: Stanford University Press.

Wirtz, J. (2015). Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy In K. Geers (Eds.), *Cyber War in Perspective: Russian Aggression against Ukraine* (pp. 29-37), NATO CCD COE Publications: Tallinn

Wivel, A. (2008). Balancing against Threats or Bandwagoning with Power? Europe and the Transatlantic Relationship after the Cold War *Cambridge Review of International Affairs* 21(3), 289-305. doi: 10.1080/09557570802253419

Woods, N. (2008). Whose aid ? Whose influence ? China, emerging donors and the silent revolution in development assistance. *International Affairs, 84*(6), 1205-1221. doi: 10.1111/j.1468-2346.2008.00765.x

World Bank. (2017). Military Expenditure (% of GDP). Retrieved from: https://data. worldbank.org/indicator/MS.MIL.XPND.GD.ZS

World Economic Forum. (2016, July). What is 'networked readiness' and why does it matter? Retrieved from:https://www.weforum.org/agenda/ 2016/07/what-is-networked-readiness-and-why-does-it-matter

Yu, E. (2013, November 25). Singapore, Seoul key players in 'Five Eyes' Spy Ring *ZDNet* Retrieved from: https://www.zdnet.com/article/singapore-seoul-key-players-in- five-eyes-spy-ring/

Yuill, J., Denning, D., and Feer, F., (2006).Using Deception to Hide Things from Hackers, *Journal of Information Warfare* 5(3), 26-40.

Zakaria, F. (1999). *From Wealth to Power: The Unusual Origins of America's World Role*. Princeton, New Jersey: Princeton University Press.

Zenko, M. (2015, August 4). The Existential Angst of America's Top Generals. *Foreign Policy* Retrieved from: http://foreignpolicy.com/2015/08/04/the-existential-angst-of-americas-top-generals-threat-inflation-islamic-state/

Zetter, K. (2016, March 3). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Retrieved by: https://www.wired.com/2016/ 03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zetter, K. (2015, January 8). A Cyberattack Has Caused Confirmed Physical Damage for The Second Time Ever. *Wired*. Retrieved from: https://www.wired.com/ 2015/01/german-steel-mill-hack-destruction/

Zetter, K. (2014, November 11). Hacker Lexicon: What's a Zero Day? *Wired*. Retrieved from: https://www.wired.com/2014/11/what-is-a-zero-day/

Zhongqi, P. (2003). US Taiwan Policy of Strategic Ambiguity: A dilemma of deterrence *Journal of Contemporary China*, 12(35), 387-407.