Sheltering from cyber insecurity?

A comparative analysis of New Zealand and Singapore

A thesis

submitted in partial fulfilment

of the requirements for the degree

of

Master of Arts in International Relations and Security Studies

at

The University of Waikato

by

Jessica Smith

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

2022

Abstract

Although there is increasing academic research on cybersecurity, very few scholars have investigated the cybersecurity approaches of small states, particularly those in the Asia-Pacific region. This thesis attempts to contribute to the ongoing discussion by analysing how New Zealand and Singapore, as two important small states in the Asia-Pacific, are seeking shelter from cyber insecurity. Drawing upon small state and shelter theory literature, the thesis begins by outlining the key concepts and arguments that guide small state behaviour in the international security environment. These theoretical and conceptual understandings are applied to New Zealand and Singapore's cybersecurity approaches. It is argued that the small states face significant resource challenges necessary to address cyber issues. Given the transboundary nature of the cyber phenomenon, it becomes apparent that domestically focused foreign policy is insufficient to attain cybersecurity. The thesis then explores the role of international and regional arrangements of strategic importance to New Zealand and Singapore to facilitate cyber cooperation. The thesis finds that larger powers, regional and international arrangements, and the use of internationally recognised rules and norms provide New Zealand and Singapore shelter from cyber insecurity. Ultimately, the nature and degree of shelter acquired is informed by New Zealand and Singapore's existing capabilities and capacity to respond to cyber threats.

Acknowledgements

Firstly, I would like to thank my chief supervisor, Dr. Reuben Steff, for providing invaluable expertise, knowledge and insights in my research journey. As well as the unwavering support and encouragement to complete this thesis.

I would also like to thank my mum for her undying love and care that allowed me to pursue postgraduate studies in New Zealand.

To my father, who always believed in my academic ability. To Bettyna, who has been my championing angel through this process.

Lastly, thanks must go to my partner Nash, for never letting me forget my potential.

Table of Contents

Introduction

The emergence of the cyber revolution has altered the global security environment and in doing so, has introduced new complexities to how state governments ensure their national security. In the contemporary security environment, digital infrastructure is increasingly the backbone for the proper functioning of the modern state across an array of governmental, economic, commercial, and social sectors. Disruption to these services in the form of direct cyber-attacks, espionage or subversion has the potential to have widespread detrimental effects. While information technology has introduced new opportunities for economic prosperity, development, and innovation, the global trend of increased dependency on cyberspace is not without significant vulnerabilities and threats. Additionally, the cyber phenomenon is transboundary, meaning cyber activity does not respect traditional sovereign boundaries.

Owing to the growing sophistication of malicious cyber activity by state and non-state actors, escalating great power competition and obstacles to global governance on cyber security issues, the stability of the cyber domain is becoming increasingly subverted. Cyberspace has become an important platform for geopolitical competition, where the most powerful states, with the most advanced capabilities and expertise, seek to exert international influence. Given there is no overarching international governance framework to regulate state behaviour in cyberspace, the exploitation of cyber tools for political or economic advancement is now a constant. For this reason, small states face some of the greatest challenges in ensuring cybersecurity as they struggle to respond economically, politically and socially to the challenges posed by larger powers and the trend towards a more competitive interstate environment. Although scholars have been investigating these broad cyber challenges to state security in the past decade, the majority of academic literature focuses on the capabilities of medium and larger powers, as well as the geopolitical competition for cyber dominance (Van der Meet, 2016). Those that have explored small state engagement in cyberspace have failed to consider the role of Asia-Pacific countries. Additionally, there is an evident lack of comparative perspectives on how small states differ in their approaches to cyber security issues, particularly between democratic and non-democratic small states. This research gap is significant and requires attention for several reasons. Firstly, the Asia Pacific region is at the forefront of cyber insecurity and contains a number of small nations. The region has the largest number of internet users globally and is home to 40% of global data centres (Iyer &

Misha, 2021). In this context, it is important to expand the knowledge on how smaller countries are responding to the cyber challenge, given the political, economic and social dependence in the domain. Secondly, it is useful to compare the approaches of different small states to establish whether the areas of similarities or differences. There is an opportunity for lessons to be learned from the best practices of one for others. As such, this paper seeks to comprehensively examine the domestic and international cybersecurity strategies adopted by New Zealand and Singapore, as two significant small states in the Asia-Pacific, to identify how, and to what degree, either state seeks *shelter* (a major theoretical concept in the small states literature that is examined in chapter one and utilized throughout the remainder of this thesis) from cyber insecurity through alliances with larger powers, international and regional institutions, and/or through adherence to and championing internationally recognised norms and rules (Thorhallsson & Steinsson, 2018). It also considers how New Zealand and Singapore, as liberal and illiberal democracies respectively, differ in their need for shelter from cyber insecurity.

Chapter one forms outlines the theoretical framework of this thesis by utilising small state and shelter theory to establish specifications for New Zealand and Singapore's foreign policy approaches to attaining cybersecurity. Understanding small state behaviour will demonstrate how having fewer resources, expertise and technological knowledge limits the diplomatic clout smaller nations have to respond to security threats. Despite this, small states do not lack agency and can leverage concepts (and the unique attributes) of smallness to influence global affairs. This analysis will adopt shelter theory to argue that given their intrinsic vulnerabilities, acquiring shelter is by default a significant component of New Zealand and Singapore's foreign policy approaches to safeguard themselves cyber insecurity. Building upon this theoretical and contextual foundation, Chapter two expands this analysis by identifying the perceptions and motivations that guide New Zealand and Singapore cybersecurity policymaking. This is achieved through an analysis of cyber threats at the international level that have implications for their national security, identifying the unique technical and political challenges that small states face in obtaining cybersecurity. It then examines the cyber landscape in New Zealand and Singapore, respectively, to determine the challenges both countries face to attain security from cyber issues and how these align with the common challenges of small states. Chapter three broadens the analytical scope by examining the ways in which New Zealand and Singapore are responding at the domestic level to cyber threats. While there are various categorical issue areas to respond to cybersecurity, this analysis focuses on investigating how these two countries are addressing the challenges of safeguarding critical information infrastructure and investments in developing a prosperous cybersecurity workforce. This analysis seeks to highlight the disparities between the two countries' approaches despite their seemingly similar attributes. Moreover, these differences inform the degree to which New Zealand and Singapore seek external shelter from cyber insecurity and it should be noted that seeking and attaining shelter, in some instances, requires states to cede an amount of sovereignty and to participate in activities that support the security interests of other states or organisation – it is not entirely cost free and requires states to balance pros and cons.

As the bedrock of New Zealand and Singapore's foreign policies, chapter four explores the role of the United Nations (UN) in facilitating cyber cooperation at the international level by examining the progress made by the UN Group of Government Experts (GGE) and Open-ended Working Group (OEWG). This chapter argues that New Zealand and Singapore's extensive involvement as small states in these UN forums has allowed a significant amount of sheltering through representation in the formation (albeit nascent) of globally recognised rules and norms in cyberspace; ensuring their interests (and that of a rules-based international community) are represented and manifested in these groups could go a long way to improving the cyber security of New Zealand and Singapore. The discussions then considers regional partnerships of strategic importance to New Zealand and Singapore; in doing so, it highlights the key ways in which they are acquiring sheltering from cyber insecurity. Chapter five investigates how New Zealand's membership in the Five Eyes (FVEY) network is a core historical and contemporary component of the country's strategic approach to providing the necessary security and intelligence to serve its national interests. Without access to the highest-quality intelligence and research capabilities afforded by its larger counterparts in the network, New Zealand could not hope to achieve its current level of security. Furthermore, this analysis considers how New Zealand attempts to balance relations with its traditional FVEY partners and the economic powerhouse, China, which is now its largest trading partner, in a way that does not damage relations with FVEYs nations or Beijing (a balance that is increasingly complicated given the trajectory towards intensified competition between China and some of the FVEY nations). As a regional leader in cybersecurity, Chapter six explores Singapore's positioning in the Association of Southeast Asian Nations (ASEAN) to facilitate regional cyber cooperation. It looks at the interdependent nature of Singapore's national aspirations to develop into a Smart Nation and the complexities of the regional environment. In doing so, this discussion explores the extensive ways Singapore contributes to securitising the ASEAN cyber landscape. The concluding remarks of the thesis reiterate the core arguments presented in previous chapters, and considers areas that merit further investigation related to cybersecurity approaches adopted by New Zealand and Singapore as small states.

Chapter One: Theoretical Framework

Introduction

This chapter establishes the theoretical framework of this paper through an amalgamation of small state and shelter theory. It begins with providing an overview of the traditional view of small states that highlights the ways in which intrinsic characteristics limit the scope of capabilities small states possess to respond to security issues comparable to its larger counterparts. The next section turns its attention to the contemporary understandings of small states that argue new concepts of image, perception and diplomacy have re-shaped their positioning in the international security environment. Lastly, shelter theory is examined to demonstrate small states can safeguard from their intrinsic vulnerabilities.

The Traditional View of Small States

Throughout the literature on small state theory, it is apparent that there is no academic consensus on what defines the 'small state'. Instead, the small state has been recognised through a 'loosely defined concept' (Maass, 2017) comprising psychological and material dimensions. While the necessary features of a state to be considered 'small' vary across the existing studies, some key recurring specifications offer a suitable basis for the analysis of New Zealand and Singapore cybersecurity approaches.

Firstly, there is consistent utilisation of terminology referring to the small state's 'lack of capabilities' and subsequent 'vulnerability'. In early studies of the small state, the measurement of a small state's relative and absolute power focused on material concepts such as population, economy (GDP) and/or territorial size (Archer et al, 2014). Scholars have suggested that small states often have a population size of up to 10 to 15 million (Vital, 1971; Armstrong & Read, 2000). Researchers argue that New Zealand and Singapore fit this traditional model. With a population of 5 million people and 0.16% share of global GDP, New Zealand encompasses a territorial size of 718,218 km² that is borderless to any other nation, ranging 15,000km of varied coastline (National Geographic, n.d; Stats NZ, 2021; Stats NZ, 2022). Although the country is rich in natural resources, it is in a remote corner of the world, remarkably distanced from neighbouring economies. Singapore - located at the juncture of the Strait of Malacca - has a similar population size of 5.6 million people, a 0.42% share of global GDP and small territorial size of 724.2 km² with access to virtually no natural resources (Department of Statistics Singapore, 2022; The World Bank, 2020; World Data, 2022).

There are unique challenges that arise from having a small population size that states must compensate for. Those with smaller population sizes have fewer personnel capable of working in administrative positions and they, therefore, often have smaller bureaucracies. Limitations on the capacity of states' diplomatic resources mean that governments and foreign ministries often lack expertise and specialisations across the full range of foreign policy issues that concern them, and this can restrict their capacity to make informed decisions (Thorhallsson & Steinsson, 2018). This can disadvantage their ability to project influence, as their foreign services are generally not as knowledgeable, qualified, and resourceful as those of larger powers (Vajvainan, 1971; Wivel, 2000). While there are small states who possess great economic strength, typically, the size of small states disadvantages them in terms of productivity, investments, resources, sectoral diversity, export dependency and risks of international economic fluctuations. For example, New Zealand and Singapore are largely trade-dependent due to the limitations of their domestic markets. The prosperity of its economies is highly dependent on a free and open trade environment that is characterised by low trade barriers and open access to capital, labour, and common currencies (Archer & Nugent, 2006; Katzenstein, 2019).

The limited resources of most small states – including relatively small amounts of finances and capital, human resources, advanced technologies, and equipment – restrict their capacity to mitigate threats and respond to security issues comparable to their larger counterparts (Wivel, 2000). Given these vulnerabilities, small states lack the capacity to exert power and/or withstand the application of power against them by larger states. This leads to adopting an 'alliance' security framework where small states seek to build alliances with more powerful states to compensate for these intrinsic vulnerabilities (Maas, 2017). These can take the form of temporary alliances that are focused on a specific threat - such as the Global War on Terror operations - or long-term, formalised and institutionalised security partnerships, such as the North Atlantic Treaty Organisation (NATO). Due to small states' vulnerabilities in the international system, issues such as entrapment and concerns for abandonment can lead to intra-alliance problems. Small states may be compelled to adopt policies and approaches on international issues in order not to displease larger trading partners and compensate for their diplomatic shortcomings (Gaertner, 2001). This draws upon the psychological dimension of small state theory, which relates to the supposedly more pragmatic views and behaviour small state leaders are compelled to adopt. In short, since smaller states recognise that they lack resources and are more vulnerable than larger ones, this forces them to be more pragmatic in their foreign policy (Keohane, 1969; Rothstein, 1968). Under this framework, small state foreign policies are entangled with those of greater powers.

By their very nature, small states share specific concerns and common interests. For this reason, they perceive that through international institutions, there is an opportunity for them to collectively advocate for norms and rules within the global system that support their security and to shape and develop an "international political culture" (Keohane, 1969). Although realist scholars claim that international institutions tend to be dominated by larger powers seeking to advance their own interests, there have been several cases where small states have achieved significant institutional influence, such as the United Nations Security Council (UNSC) agenda. During Estonia's rotating Presidency of the UNSC, a key initiative for its diplomats was to raise awareness of cyber threats against international peace and security. In doing so, Estonia successfully organised the first UNSC formal meeting on cybersecurity held in June 2021, known as the UNSC Debate on Cybersecurity: Maintaining international peace and security (Bloomberg, n.d). The strong initiative, guided by Estonia's leadership, represents a good example of how a small state can make an influential impact in foreign affairs. However, as Baldur Thorhallsson (2012, p.157) explained, "a state's perceived neutrality is not automatically transformed into an asset for international influence. In order to become an asset, it must be combined with image-building and factors such as experience and skills, which take time, leadership and initiative to develop". This connects to the contemporary understandings of small states, which the following section outlines.

Contemporary understandings of small states

In the contemporary small state studies (considered to be those that followed the end of the Cold War), new concepts were introduced – including the role of perception and image, administrative competence, favourable diplomatic multilateral arrangements - which have been incorporated in the understanding of small state behaviour (Thorshallsson, 2012). To compensate for their scarcer diplomatic resources, small states often must take a strategic approach to prioritise policy initiatives that support their national goals. Small states can assert influence in pivotal moments and areas that affect aspects of the global order by upskilling their administrative competence and utilising strategic diplomatic skills in specific policy areas. In doing so, they can distinguish themselves as a favourable partner to larger counterparts and gain greater opportunities to make global contributions (Thorshallsson, 2012). For example, New Zealand has demonstrated compelling leadership in several aspects of international governance for its specialised strengths in Pacific affairs, disarmament, non-nuclear proliferation, climate change, environmental policies and indigenous rights (Burton, 2019).

Although small states are commonly observed as intrinsically weak, through multilateral and bilateral networks, the notion of 'smallness' may offer some advantages for these states. Alan Chong (2010) argues that "smallness, being geographically limited, can be psychologically tactical in disarming major powers' suspicions of the small state's motives. On the other hand, as some have argued, the small state's foreign policy apparatus may possess among its human resources intellectual and propagandistic skills that are disproportionate to its physical size. These resources function as compensatory symbolic power". Moreover, as these states usually cannot rely on the exercise of decisive power, they often emphasise the importance of strong diplomatic relations, favourable global reputations, and multilateral cooperation. These qualitative and subjective features, if harnessed, allow small states to amass and use soft power in the international system to overcome issues that they cannot resolve on their own (Nye, 1990). This relates to the fact that, in global affairs, the way in which states perceive one another is significant; through diplomacy, there is an opportunity for states to shape their image and reputation in the international system.

New Zealand's global reputation links to the fact that it is one of the least corrupt countries in the world, with substantial social capital, a world-class education system, and a committed social welfare system that underpins social stability and cohesion (Brady, 2019). Despite its territorial location in a remote corner of the world, New Zealand - as a liberal democratic, multicultural, post-colonial state - has a significantly high level of international participation and interest (Brady, 2019). Similarly, Singapore, as an illiberal democratic country, benefits from a positive image disproportionate to its physical size. The nation is considered a leading nation in economic globalisation and consistently ranks among the world's top five most competitive states (Statista, 2021). This reflects its government's strategic decisions to extend its international value through soft power measures in regional and global partnerships (Chong, 2010). Both New Zealand and Singapore rank highly on soft power metrics. The USC Center of Public Diplomacy's 'Soft Power 30' listed New Zealand as 17th while Singapore ranked 21st in 2019 (Portland, 2019).

Having discussed the intrinsic structural weaknesses of the small state, this chapter now outlines how shelter is acquired to overcome these vulnerabilities.

Shelter Theory

Shelter theory is a theory of small state behaviour. Due to the intrinsic vulnerabilities small states face and their vastly different needs, shelter theory seeks to explain how small states operate according to different logistics than larger states. To compensate for their vulnerabilities, small states seek what is referred to as 'shelter' from larger powers, international institutions, or the use of internationally recognised norms and rules. The prosperity and survival of the small state depend on the nature and amount of shelter they can attain. Shelter theory focuses on three interrelated common challenges to small states: "the reduction of risk before a possible crisis event; assistance in absorbing shocks when risk goes bad, and help in recovering after such an event" (Thorhallsson & Steinsson, 2018). Small states seek shelter to address each vulnerability through political, economic, and societal means.

Political shelter

Given that small states have less political clout than larger states as previously discussed, regional and international institutions are a means to overcome diplomatic vulnerabilities. The asymmetry in political and economic power that states face in negotiations can be reduced by shifting negotiations from the anarchical nature of the international system to institutions governed by global rules and norms. By giving them formal votes and requiring their participation in final negotiations to validate outcomes, organisations formalise the say and opinions of their smallest members (Thorhallsson & Steinsson, 2018). For example, the UN is considered the centrepiece of global equalising; by indoctrinating sovereign equality through one state, one vote, where small states theoretically have the opportunity to contribute and participate in international affairs with a disproportionate influence to its size, and economic capabilities. Half of UN members are small states. (Brady, 2019; Panke, 2012).

Robert Keohane and Lisa Martin (1995) argue that international organisations provide access to information (research and analysis), reduced transaction costs, improve commitments' credibility, and form focal points for coordination and cooperation that would otherwise be unattainable for small states. These can help small states to improve the quality of public goods available to their people and modernise their bureaucracies. Moreover, international organisations allow small states unique opportunities to build relations with a range of additional states than possible through bilateral relationships, to obtain recognition of their independence, and forge a better status in the international community. All of this is necessary for small states to receive shelter from states with larger diplomatic clout (Thorhallsson & Steinsson, 2018).

Economic shelter

As Thorhallsson & Steinsson (2018) explain, "economic shelter can take the form of favourable market access, direct economic assistance, beneficial loans, assistance with fiscal management, and currency unions etc". Through a unilateral reduction in trade barriers, small states can reduce some of their vulnerability - but this is dependent on stable access to large markets and positive relationships with larger states to maintain that access. While the liberalisation of free markets is beneficial for all states, small states arguably gain the most, given they cannot rely on the large domestic markets afforded to large states. As heavily-trade dependent, small states need access to external markets, which is only achievable by establishing trade relationships with other countries. Access to open and stable foreign markets is a relatively new development but has eased through government initiatives to form bilateral and multilateral trade agreements (Thorhallsson & Steinsson, 2018). The General Agreement on Tariffs and Trade and the World Trade Organisation have played critical roles in the global liberalisation of the trade environment. Technological advancements in communications and transportation have also helped small states access more markets by reducing small state vulnerability, such as the cost of distance to trade (Eaton & Kortum, 2002).

International economic stability is crucial. Since small states are largely trade-dependent and have low sectoral diversity, they are at greater risk of economic crises from international fluctuations. The loss of a market or unfavourable price changes can be detrimental for small states, at least in the short term, until new trade relations are established. Large states do not carry this burden. If the global economy has a crisis, larger states still have regional and sectoral diversity to compensate for these losses and better means to economically recover relatively on their own. When there is a crisis in the central sector of the small state economy, the economic consequences are felt on a national scale. In these instances, small states may need to seek external assistance. Small states that do not have these external insurances are at risk of more drastic economic busts (Alesina & Spolaore, 2003, p.4). Whether in the form of loans or direct aid, foreign assistance depends on small states successfully establishing relations with large states and international institutions. The nature of these relationships determines the timeliness and conditions for favourable assistance (Thorhallsson & Steinsson, 2018).

<u>Societal shelter</u>

While small state theory has primarily neglected social and cultural aspects, shelter theory suggests that society can evolve through interaction with other ideologies, cultures, and ideas. Removing barriers between the small state and the rest of the world facilitates access to new technology, innovations, culture, and ideology. This allows old, inferior structures to be improved or replaced. (Rokkan and Urwin, 1983, p.4). Innovation is facilitated through connections to external knowledge and expertise. Although the world is becoming increasingly interconnected, small states face ideational limits. Small states depend on the free flow of ideas with the outside world to prosper. As explained by Thorhallsson & Steinsson (2018), "small communities cannot generate the same flourishing bank of innovative ideas as compared with bigger societies and, thus, need both societal (cultural) access and cover provided by larger communities".

Conclusion

While the literature on small state behaviour has evolved since World War II, both traditional and contemporary understandings provide helpful insight into New Zealand and Singapore's cybersecurity approaches. In short, small states have limited diplomatic clout, fewer human resources and economic capacity to mitigate and respond to security issue threats comparable to more powerful, larger nations. These restricted material concepts are explored in later chapters to demonstrate how small states continue to fall behind in acquiring the necessary clout to mitigate and defend themselves from cyber insecurity. Contemporary specifications of imaging, perception and diplomacy are utilised in the context of small state success in acquiring favourable partnerships with more powerful states to safeguard from cyber threats.

Furthermore, shelter theory argues that the recognition of their intrinsic vulnerabilities shapes small state behaviour in the international security environment. By acquiring shelter from larger powers, regional and international institutions, or the use of global rules and norms, small states can compensate for these structural weaknesses. Small state survival is dependent on the nature and amount of political, economic and social shelter they can acquire.

The importance of the above is to establish the theoretical framing for further analysis of New Zealand and Singapore policy approaches to cybersecurity in proceeding discussions. The next chapter turns the attention of this analysis to the extent of the cyber phenomenon on national security and the challenges small states face in acquiring cyber security comparable to larger states.

Chapter Two: Threats of the cyber phenomenon to small states

Introduction

Since the turn of the century, the growing omnipresence of information technology has become integral to conventional security, nontraditional warfare and societal security. Growing sophistication of cyber-attacks, escalating great power competition, and diverse perspectives on global cyber governance have increasingly undermined the stability of cyberspace. This chapter seeks to provide the reader with a comprehensive understanding of how the small state's political, economic, and social stability is being threatened by the emergence of new complex cybersecurity issues. This is achieved by first examining the power of cyber threats to undermine national security, highlighting the potential for cyber mechanisms to be leveraged as an influential political tool in global affairs. The second section considers small states' technical and political challenges to achieve security in the cyber domain compared to larger counterparts. Lastly, this chapter examines the impact of cyber vulnerabilities in New Zealand and Singapore, respectively. The overarching argument of this chapter is that small states are increasingly vulnerable to cyber threats due to the unique challenges they face in acquiring security. Furthermore, these weaknesses are apparent in New Zealand and Singapore.

Cybersecurity threats to national security

Central to the world's rising digital economy, the Indo-Pacific region is at the forefront of such cyber insecurity where New Zealand and Singapore reside. According to the IBM's annual X-Force Threat Intelligence Index, the Asia Pacific was the most targeted geography in 2021 with a 26% share of global cyber-attacks against the region. For the first time since the IBM report began reporting geographic trends, the Asia Pacific surpassed Europe and North America (IBM Security, 2022). Since the onset of the Fourth Industrial Revolution, the region has prospered from economic opportunities; however, its increasing dependency on Information and Communication Technology (ICT) has exposed it extensively to enhanced threats and vulnerabilities (Segal et al, 2020).

Many modern countries are now highly cyber dependent, with increasing reliance on digital services and platforms by civil society, business sector and government. Disruption of these services can give rise to widespread diplomatic, economic, and societal damages. Diversity of attackers further complicates cyber affairs and potential effects, state actors and non-state actors such as terrorists or criminals alike can leverage cyber tools to advance their political or profit-driven goals further. There is a wide range of cyber threats, including war, terrorism, espionage, sabotage, disruption, and crime (Lan, 2020). Considering the cyber domain is imperative to understanding how states formulate their national interests in the contemporary security environment. Governments are faced with the need to maximise cyber opportunities – surveillance intelligence-gathering tools, enhancing information infrastructure, societal connectivity – while mitigating complex threats. As the possibilities for information technology innovation grow, consequently, so does the prospect of competition and conflict.

In 2009, former United States (US) President Barak Obama said, "it's the great irony of our Information Age – the very technologies that empower us to create and to build also empower those who would disrupt and destroy" (Barak, 2009). Due to the cyber phenomenon's dynamic and expeditious nature, policymakers are often playing catch up in effectively responding to the risks and threats. Since the US Department of Defense officially incorporated cyberspace as the fifth domain of warfare (alongside sea, land, air, and space) in 2011, there have been growing concerns that the cyber domain is becoming militarised (Wagenseil, 2011). Additionally, increasing state investment in offensive cyber capabilities has led to a new cyber arms race. Adversaries utilising cyberspace for their geostrategic purposes lie at the heart of governmental concerns as the amount of malicious cyber activity by or supported by nation-states continues to rise (Manantan, 2021).

Widespread adoption of information technologies underpins the effective functioning of the modern state. In this, critical infrastructure is profoundly interconnected and interdependent with ICTs. The cyber threat, which includes the possibility of degrading state functions and subversion to these systems, is of significant concern to those authorised to establish, maintain, and secure them. In Singapore's 2021 Cybersecurity Strategy, it is stated that "growing cyber-physical risks as cyber disruptions can spill over to the physical domain; ubiquitous digital connectivity that expanded the attack surface; and increasing geopolitical tensions in cyberspace" (CSA, 2021a, p.7). Cyber threats can virtually instantaneously transcend traditional state boundaries, unlike conventional domains (the sea, land, and air); no geographical limit may constrain their effects. Since malware travels through a virtual medium, it can easily cross numerous jurisdictions and grants an exorbitant degree of anonymity to attackers (Kello, 2013). In the absence of overarching governance or legal framework to regulate state activity in cyberspace, there remains a lack of knowledge, and threat intelligence sharing that limits transparency among states. The swift sharing of cyber threat information and data is essential to effective deterrence and policy responses to cyber incidents (Kearney, 2018). Sophisticated cyber intrusions and attacks against core infrastructure - to infiltrate critical elements of a state's society and ability to govern - can inflict significant costs and damage a state's national security and economic prosperity (Stevens, 2012). Cybersecurity Venture predicts global cybercrime damages will hit $6 trillion annually by 2021, and global ransomware damage costs will reach $20 billion in 2021 - up from $11.5 billion in 2019 and $5 billion in 2017 (Morgan, 2019).

While the financial costs of cyberattacks are often high, indirect costs - loss of life, loss of public trust and confidence - can be significantly higher. Preserving the public's confidence is critical to the legitimacy of a government, particularly during the management of the current COVID-19 pandemic and the rebuilding that follows (Koh, 2020). Political subversion of political processes to exert influence is a growing concern, that goes beyond the attacks we see against critical infrastructure. As cyberspace grants a high degree of anonymity and direct access to targets, cyber tools and technologies facilitate more successful and persuasive political warfare campaigns. These campaigns represent a significant existential threat that undermines the independence, beliefs and values of a respected state (Paterson & Hanley, 2020).

Given that democratic processes function on a certain level of transparency, subversion is particularly damaging to the political legitimacy of democratic nations. Even more concerning is that some successful campaigns are never discovered or exert influence for an extended period before being uncovered (Omand, 2018). While cyber-attacks and espionage can cause significant technological, informational and financial loss, it does not have the potential to hinder political legitimacy in the way political subversion does.

Small state cyber security: technical and political challenges

Unique challenges face small state policymakers at the technical level of cybersecurity. During the 2017-2019 period, the 13 countries with the highest percentage of Internet users per capita were micro or small states: Bahrain, Qatar, Liechtenstein, Kuwait, United Arab

Emirates, Iceland, Bermuda, Denmark, Norway, Faroe Islands, Aruba, Luxembourg, and Monaco (The World Bank, 2019). Having heavy reliance on ICTs that underpin the operational functions of core infrastructure arguably intensifies risks. A report by McAffee (2012) suggests that "the less sophisticated and widespread a country's connection to the internet, the lesser the cyber-threat. The more services are online, the higher the risk of cyber-attack". Small states with high rates of internet penetration are particularly vulnerable to threats. According to NordVPN's latest Cyber Risk Index (2020, p. 3), the majority of states with the greatest vulnerability to cybercrime are small states; New Zealand and Singapore ranked in the top 10 countries most at risk. Additionally, larger powers have numerous internet exchange points and/or very large IXPs, whereas typically, smaller states have only one exchange or no IXP at all. As such, the domestic connectivity of small states is greatly dependent on international data circuits (Stapleton-Gray & Woodcock, 2011).

On the other hand, it is argued that asymmetry affords small states with particular advantages in cyberspace to counter the military advantage of more powerful states. Asymmetric advantage is based on Joseph Nye's (2011, p. 20) assumption that "the barriers to entry in the cyber domain are so low that non-state actors and small states can play significant roles at low levels of cost". Nye maintains that the necessary operational and technical expertise to carry out cyber-attacks are easily accessible by utilising hacking communities, cybercriminal markets, and commercial satellite imagery (Domingo, 2016). However, an analysis of global cyber activity suggests that this assumption is relatively inaccurate in practice, as advanced cyber capabilities so far have enhanced the power of larger states against small states. Most malicious cyber-attacks have originated from larger, more powerful adversaries. According to Robinson's research, China is responsible for 28.6% of the world's total cyber-attack, followed by Russia (27.2%), North Korea (11.6%), Iran (11.2%), and the US (4.3%) (Robinson, 2021). Some cyber-attacks are extremely sophisticated. For example, the US developed Stuxnet virus against Iranian nuclear centrifuges. This virus is regarded as one of the most sophisticated cyber capabilities to have ever been developed, and it demonstrates the substantial cyber power of the US. The complexity and scope of the attack reflect America's technological leads across numerous areas of expertise, including covert intelligence operations, computer science, and electronic and nuclear engineering (Lindsay, 2013). These types of expertise are not easily accessible for small states, primarily when relevant cyber knowledge and operational training reside in the most powerful countries (Domingo, 2016).

Major powers have increasingly invested in the development of offensive cyber security capabilities. As expressed by Dr. Mike McGuire (2021a), "nation-states are devoting significant time and resources to achieving strategic cyber advantage to advance their national interests, intelligence gathering capabilities, and military strength through espionage, disruption, and theft". The cyber domain has become a fundamental component of global influence; a battleground between the greatest cyber powers, China, Russia and the US, is underway. This strategic rivalry may define the global norms and agreements that are developed and implemented in the international system. Powerful states are increasingly developing offensive cyber capabilities to compete for military dominance (Domingo, 2016). Cybersecurity spending among the major powers is projected to grow between 2019-2021, by 11% in the US, 25% in China through to 2023, and by up to 200% in Russia through to 2023 (McGuire, 2021b). Notably, US President Joe Biden's recent discretionary funding requests for 2022 outline a 1.5 trillion budget to finance investments in federal technology and cybersecurity, including $769 billion in non-defence discretionary funding - a 16% increase from the 2021 approved funding (Executive Office of the President, 2021). It seems plausible that given that powerful states spend the most on their cyber capabilities and have the greatest human cyber expertise, small states will continue to fall behind.

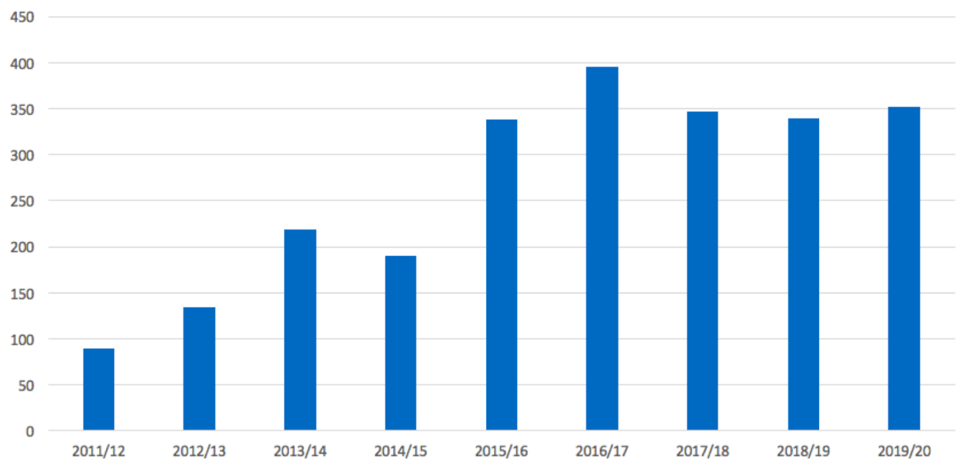
Large powers have already demonstrated their willingness to utilise their enhanced cyber capabilities in disputes and conflicts with smaller, weaker nations. The ongoing Russian-Ukraine conflict is a crucial example of such claims. A recent report released by Microsoft found that since Russia invaded Ukraine on 24 February 2022, a multitude of Russian cyber threat groups has conducted malicious activity in support of its military's tactical and strategic objectives. It was revealed that military missiles or ground attacks appeared to be coordinated in tangent with computer network operations against a shared target. These cyber operations sought to disrupt the Ukrainian government's ability to disseminate intelligence and secure core infrastructure, further substantiating the disparity in cyber capabilities between small and large nations (Microsoft, 2022). Even more alarming for small states is the increasing use of widespread political warfare campaigns by larger powers – notably Russia and China –to exert influence on the domestic policies of their target state/s. One of the most well-known examples of political subversion is Russia's systematic success in interfering with the 2016 US presidential elections. A joint 2017 report by the CIA, FBI and NSA confirmed that "Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency" (Office of the Director of National Intelligence, 2017, p. 7). If we consider the substantial cyber power of the US, how would small states fare in a similar situation? Arguably, small states lack the technological resourcing and expertise to withstand influence power comparable to their larger counterparts.

One of the ways in which small states can overcome the limitations of their intrinsic vulnerabilities is through regional and international platforms. In theory, these institutions and organisations afford a higher degree of influence for small states than otherwise attainable by establishing rules and norms that foster cooperative approaches to international security issues. Throughout the last decade, regional alliances and international institutions have worked towards developing cooperative efforts to address cyber security issues. In the absence of coherent international cooperation, criminal safe havens remain, and gathering forensic evidence in the aftermath of a cyberattack is difficult (Kello, 2013). Later in this report, the progress made by the UN, ASEAN and FVEY toward cultivating regional and international cyber cooperation will be discussed. Furthermore, this analysis will identify empirical evidence that suggests New Zealand and Singapore have sought shelter from cyber insecurity through these regional and international efforts.

New Zealand’s cyber landscape

New Zealand is experiencing increasing cyber security incidents against organisations of national significance or cyber threats that have the potential to undermine New Zealand's economic wellbeing and national security, with 30% of New Zealand Cybersecurity Centre's (NCSC) cyber incidents linked to state-sponsored actors during 2019/20 (NCSC, 2020). While this represents a smaller fraction than the 38% of state-sponsored links found in 2018/19, state-sponsored actors are increasingly looking to obfuscate their malicious online activity by making it more difficult to distinguish between legitimate cyber activity and cybercrime (NCSC, 2019).

Figure 1. Cyber security incidents recorded in New Zealand 2011-2020



Note. Data sourced from the New Zealand National Cyber Security Centre (NCSC). "NCSC incidents either involve organisations of national significance, or cyber threats that may affect New Zealand's national security and economic wellbeing". (NCSC, 2020, p. 15).

The 2019/20 NCSC Cyber Threat Report (p.15) concluded that "New Zealand's nationally significant organisations continue to be frequently targeted by malicious cyber actors of all types." Since the NCSC only reports on nationally significant organisations (NSO), the data are shown in Figure 1 only represents a small proportion of New Zealand cyber security incidents. For example, New Zealanders (individuals, small businesses, and large organisations) reported 7,809 incidents to CERT NZ in 2020, a 65% increase from 2019 (CERT NZ, 2020). In addition, a recent Reserve Bank bulletin reported that the approximate annual cost of cyber incidents is around NZD 142 million for the New Zealand banking and insurance industry (Collins et al., 2020).

Additionally, more systems, businesses, and individuals have moved online in response to the global COVID-19 outbreak. It has created many opportunities for malicious cyber actors to commit data breaches, perpetrate financial crimes, carry out espionage activity or disrupt the online services of organisations, specifically those with a pandemic response position. In August 2020, Government Communications Security Bureau (GCSB) Director-General Andrew Hampton (2020) warned that "New Zealand domains and organisations could possibly be added to the net of potential targets owing to increased global media reporting on, and interest in, New Zealand's response to Covid-19". Since Hampton's speech, several key organisations, including the New Zealand Stock Exchange (NZX), Reserve Bank of New Zealand, Waikato District Health Board, and the Health Research Council have been subject to disruptive ransomware and cyberattacks (NZ Parliament, 2021). During the September

2020 NZX cyber-attack, its operational website was taken offline over four days, and trading was severely disrupted. Following the attack, the Financial Markets Authority (2021) released an obligation targeted review that found:

- NZX did not have adequate technology capability across its people, processes and platform to comply with market operator obligations and especially in the context of its systemic importance.
- NZX was aware of the capacity limitations of its core back-end processing system, particularly as daily trading volumes had increased in the last three years.

Given the national importance of the infrastructure that NZX provides, it is concerning that the exchange knowingly failed to meet its obligations to have sufficient technological capabilities, including low levels of resourcing, inefficient processes, and weak risk and crisis management. However, it is not necessarily surprising given New Zealand's positioning as a small state with limited human resources and capacity to adequately provide for the necessary cybersecurity expertise and resourcing. The NCSC cyber security assessment of data gathered from 250 New Zealand NSO's reported that only 19% of organisations have a dedicated Chief Information Security Officer, and 39% do not provide cyber security reporting to senior management (NCSC, 2018). Head of cybersecurity at IT consultancy Thetha, Jeremy Jones argued that,

> There's a reason why New Zealand is a very juicy target. The country is highly digitized and so dependent on the internet and cloud services. But historically, we're at least 10 years behind the U.K. and Europe on general cyber-security measures in the commercial space" (Insurance Journal, 2021).

New Zealand faces substantial resource challenges to strengthen its cyber security, which aligns with the common challenges of small states in the security policy sector. A 2021 New Zealand survey by ISACA found that: 66% of respondents say their cybersecurity teams are understaffed (compared to 55% globally); 59% have unfulfilled cybersecurity positions (versus 55% globally), and 52% say their cybersecurity applicants are not well qualified (versus 50% globally) (Putt, 2021). In a speech by Andrew Hampton (2019), it was openly acknowledged that the GCSB operates within legislative and resource constraints that it operates under.

There is also difficulty retaining highly specialised ICT specialists in the public sector and securing ICT professionals in New Zealand when many countries overseas offer competitive pay. The 2021 Digital Skills Aotearoa report uncovered that almost one in five IT professionals change roles annually. While all industries expect some staff turnover, this high rate demonstrates the particularly acute problem for New Zealand (Williams, 2021). Owing to New Zealand's constraints in terms of cyber capabilities and capacity, New Zealand continues to rely on its international partners for intelligence. An Independent Review of Intelligence and Security in New Zealand found that "the benefits New Zealand derives from its international intelligence sharing and cooperation arrangements by way of the transfer of technology, skills and expertise is valuable for a country of our size and limited resources" (Cullen & Reddy, 2016, p.58).

Singapore's cyber landscape

As a small state with very few natural resources, Singapore has to be innovative to build its economy and enhance its growth strategy. Despite its physical limitations, the country has become one of the most developed and wealthiest nations in the world by pursuing its Smart Nation strategy (Smart Nation Singapore, 2018). The initiative aims to utilise technology and connectivity to empower the lives of Singaporeans, create greater economic opportunities and improve the nation's growth prospects in the region. The nation's positioning as a trusted, secure and transparent global Infocomm hub has accompanied unique global risks in the form of hacking, cyberattacks, and cyberterrorism. These threats relate to Singapore's ability and ambition to "attract, process, coordinate and circulate global information and data flow" (Heng, 2016, p.191). Government leaders consistently engage in speech acts to address the gravity of security threats. Speaking at the 2018 Singapore International Cyber Week, Deputy Prime Minister Teo Chee Hean (2018) warned that,

> "Cyber-attacks are no longer a question of if, but when and how far or how deep they can get in our systems. Cyber-attacks are also causing more serious harm, by disrupting essential services, blocking access to critical information and even shutting down government agencies."

At the Singapore International Cyber Week 2020, UN Under-Secretary-General Izumi Nakamitsu acknowledged that the UN considers Singapore a global leader in cybersecurity (The Strait Times, 2020). Despite this, Singapore's cybersecurity landscape remains fraught with malicious cyber activities; recent significant growth can be attributed to leveraging the COVID-19 outbreak.

Figure 2. Cyber threats reported in Singapore 2016-2020

	Ransomware	Phishing Websites/URLs	Cybercrime
2016	19	2512	691
2017	25	24,420	5430
2018	21	16,100	6215
2019	35	47,500	9430
2020	89	47,000	16,117

Note. Data sourced from Cyber Security Agency of Singapore.

As a result, 2020 saw a sharp rise in the number of malicious ransomware and phishing cases reported to the Cyber Security Agency of Singapore (CSA); 89 ransomware cases, a significant increase of 154% from 2019; and 9,080 phishing cases handled by the CSA from 8,491 in 2019 (CSA, 2021a). In addition, a 2018 Microsoft study revealed that the likely economic damage owing to cybersecurity incidents in Singapore could reach an astounding US$17.7 billion, 6% of Singapore's total GDP (Singapore News Center, 2018).

Singapore was ranked the country most committed to cybersecurity by the International Telecommunications Union in 2017. However, the following year SingHealth IT systems - Singapore's most prominent health database - was the target of a significant cyber-attack. Personal medical details of 1.5 million patients were illegally accessed and copied, representing the most severe personal data breach in Singaporean history. Notably, attackers systematically and repeatedly targeted Singaporean Prime Minister Lee Hsien Loong's records. The Cyber Security Agency (CSA) of Singapore determined that the attack was the work of an Advanced Persistent Threat group, which refers to sophisticated cyber attackers, typically a nation-state or state-sponsored (Iswaran, 2018). The attack's implications were severe and reinforced Singapore's longstanding concerns that cyberattacks could target critical infrastructure and essential services. Moreover, the fact that attackers distinctly targeted President Lee's data adds to the severity of the attack. Following the incident, Mr S Iswaran (2018), Minister-in-Charge of Cybersecurity acknowledged that,

> We will do our utmost to strengthen our cybersecurity. *But it is impossible to completely eliminate the risk of another cyber-attack*. This is an ongoing battle with potential cyber attackers who are constantly developing their capabilities and seeking out new vulnerabilities.

Solicitor-General Kwek Mean Luck found that iHis staff became aware of unauthorised access attempts on SingHealth's network over a month before reporting the incidents to senior management. Moreover, the failure to timely report the data breach to the Ministry of Health and CSA violated the CSA's National Cyber Incident Response Framework. Despite extensive investment in Singaporean cybersecurity capabilities and policies, people often remain the weakest link in any cyber defence. For example, Singapore's Safer Cyberspace Masterplan 2020 (NCSM2020) found "only 4% of survey respondents could correctly identify phishing emails from legitimate ones, less than 2 in 5 Singaporeans feel that such malicious cyber activities would happen to them, and more than half of digital enterprises in Singapore have no cybersecurity measures in place" (CSA, 2021b)

Singapore is ranked the second-best city globally for cybersecurity professionals in terms of salary, job vacancies, and cost of living (Walstad, 2021). However, its most significant challenge to cybersecurity defence subsists in the lack of cyber security professionals and employees with appropriate skills in the workforce. According to the National Cyber Security Master Plan 2018 (NCSM2018), less than one percent of Infocomm practitioners work in cybersecurity. In 2020, (ISC)^2 Cybersecurity Workforce Study established that Singapore's currently estimated cybersecurity workforce is 57,765, with the size of the workforce gap at 17,972. To address the human resource challenges, Singapore heavily invests in its domestic cyber capacity to increase the workforce and cybersecurity progressions in the Infocomm sector (ISC^2, 2020).

Conclusion

Modern countries are becoming increasingly networked. Information technologies underpin the functioning of core critical infrastructure, and there is heavy reliance on the digital flow of goods and services for economic prosperity. While the emergence of the cyber domain represents new opportunities for economic development, transparency, and communication, the challenges and threats of cyberspace to state security have become profound. These can degrade state functions, political subversion, or direct financial costs. While attaining cybersecurity against complex, evolving threats is a challenge for all countries, why is the issue more acute for small states?

Firstly, given its intrinsic lack of capabilities, cyber expertise, resources, and technical training are not as easily accessible for small states comparable to larger, more powerful adversaries. Although there are arguments that suggest the low cost of entry into the cyber domain facilitates greater participation for small states, there is tangible evidence that suggests this is not as accurate in practice. As cyberspace becomes increasingly militarised as a political tool for global influence, major powers lead in the development and investment of offensive cyber security capabilities. The majority of malicious cyber activity has originated from larger states with proven sophistication in cyber expertise. Powerful states have not been shy to exert cyber dominance and advanced capabilities against smaller nations during disputes and conflicts. Given that larger states have greater human cyber expertise and financial spending in cyber capabilities, it is plausible that small states will continue to struggle in comparison. Owing to the transboundary nature of information technology and cyber domain, these challenges inform cybersecurity policy-making approaches of small states.

New Zealand and Singapore are experiencing significant growth in the number of attacks linked to the international environment's increasingly interconnected and interdependent nature. More worrying, these incidents include sophisticated attacks, increasingly by state-sponsored actors that target nationally significant organisations that underpin the governing of New Zealand and Singaporean society. While both nations share similar resourcing constraints aligned with common challenges of the small state, Singapore has built greater expertise and reputational standing in the cyber sector than New Zealand. The next chapter investigates the ways in which New Zealand and Singapore are seeking to address the issues of cyber threats at the domestic level.

Chapter Three: Responding domestically to cyber threats

Introduction

Building upon the previous chapter, this analysis will provide an overview of the domestic measures New Zealand and Singapore are implementing to mitigate cyber threats. There is a range of categorical issue areas addressing cybersecurity. For the purposes of this analysis, priority will be given to investigating how New Zealand and Singapore are respectively addressing the challenges of safeguarding critical information infrastructure and investments in developing a prosperous cybersecurity workforce. It is hoped that this discussion provides the reader with an understanding of how New Zealand and Singapore, as small states, are implementing domestic measures to mitigate cyber threats. Furthermore, by discussing the different issue areas parallel to each state, it seeks to highlight some of the key ways the two countries differ in their approaches despite their relatively similar attributions that will be discussed in the conclusion. These differences inform the degree to which sheltering is required from cyber insecurity and will be looked at in the following chapters.

New Zealand

Safeguarding Critical Information Infrastructure (CII)

Former New Zealand Prime Minister Robert Muldoon approved the development of the GCSB in 1977 as part of the SIGINT intelligence with the FVEY network that will be explored at length later (GCSB, 2022). In the contemporary security environment, the GCSB safeguards the cyber and intelligence interests of New Zealand from malicious cyber activity. This is achieved by gathering, analysing and reporting fundamentally on foreign intelligence - that aligns with government policies - to support government decision-making (Hampton, 2020). The GCSB administers cybersecurity and information assurances of CII services for both the private and public sector. It was only in 2011 that the New Zealand's NCSC was launched to support the existing efforts of the GCSB. Operating within the GCSB, the NCSC is responsible for providing incident response through advisory services, support and education to organisations of national significance from cyber threats (Barker, 2021).

In August 2013, the New Zealand Parliament passed the GCSB and Related Legislation Reform Bill that reshaped the existing role of the GCSB from its formerly foreign-focused cybersecurity to the broader domestic environment. The bill established a legal basis for the agency to intercept digital communication between New Zealand citizens and permanent residents (NZ Parliament, 2013). These reforms were met with heavy public criticism around the government's role in accessing private communication between New Zealanders. The New Zealand Government made efforts to ease concerns, including a personal emphasis by acting Prime Minister John Key (2013) that "the bill requires GCSB to get a warrant from the independent Commissioner of Security Warrants and me before it can intercept a New Zealander's communications. That warrant must be issued for a particular function, in this case, cyber security. The clear intention of that function is to protect, not spy". Despite these assurances, the New Zealand public remained sceptical, highlighting the difficulty in finding the balance between privacy and security in the cyber domain. While this issue cannot be generalised to all small states, it sets forth a potentially interesting dilemma that liberal democratic small states may suffer from specifically due to their national values of freedom.

To address the cyber domain's ever-evolving threats, the GCSB developed CORTEX in 2013. The CORTEX system is New Zealand's central suite of cyber defence capabilities provided to organisations of national significance to counter cyber threats. The emphasis of the tool is to counter technologically sophisticated foreign-sourced malware. CORTEX involves the implementation of defence capabilities by the GCSB to detect and disrupt advanced malware. While the GCSB does not disclose organisations receiving the CORTEX defences for security reasons, generally, these include government departments, niche exporters, critical economic generators, research institutions, and operators of critical national infrastructure in the public and private sector (GCSB, 2017a). Closely linked to CORTEX, the Malware-Free Network (MFN) initiative went live in June 2021. The initiative involves the GCSB sharing cyber threat intelligence with various consenting CIIs to help protect them against cyber-attacks. The MFN provides near real-time threat information of current malicious cyber activity targeting New Zealand entities as threat detection and disruption service. Unlike CORTEX, it is more widely available to organisations of national significance through cybersecurity providers or network operators (GCSB, 2017b). However, it is important to note that the use of these governmental tools is not enforced and requires voluntary adoption by the organisations involved.

Since 2013, the Cyber Security Emergency Response Plan (CSERP) has informed New Zealand's response to cyber security emergencies. It is overseen by the Department of the Prime Minister and National Cyber Policy Office. CSERP is a framework to guide the government's response to a cyber security emergency - an incident that results in serious or sustained disruption to digital infrastructures crucial to New Zealand's health and safety, economic-well being, democratic institutions or international reputation - to ensure government agencies and officials understand their role in such an event, the private sector understands the government's approach, a coordinated and effective response, and swift restoration of operations (Department of Prime Minister and Cabinet, 2021).

In May 2016, then Minister for Communications, Amy Adams, announced an investment of $22.2 million on a newly established national Computer Emergency Response Team (CERT) to advance New Zealand's cybersecurity capabilities to tackle cyber-attacks and cybercrime. CERT NZ resides within the Ministry for Business, Innovation and Employment. The national CERT has three primary functions: analysing the international cybersecurity landscape for relevant threats and risks to New Zealand and providing security updates based on the information ascertained; acting as a central platform to report cyber incidents, providing expert advice to manage the impacts from the attack, and raise awareness on cybersecurity best practices. By establishing a national CERT, New Zealand joins a global network of CERTs - AusCERT (Australia), HKCERT (Hong Kong), and US-CERT (the United States) - to collaborate on cyber incident reporting and improve the nation's access to information on potential or real-time cyber-attacks (Adams, 2016; Barker, 2021).

Investing in a strong and capable cybersecurity workforce

Industry-oriented curriculum

In 2014, ICT Graduate Schools were established in Auckland, Wellington, and the South Island to provide graduates with relevant work experience and business-focused expertise. As part of New Zealand's Cyber Capability goal under the New Zealand Cyber Security Strategy (2019), the Cyber Security Skills Taskforce was established in 2016 to address the shortage of cyber professionals in New Zealand. In response to industry pressure for junior cyber security employees that could be trained more quickly than with a standard tertiary degree, a Level 6 Diploma was developed at the advice of the task force (Faafoi, 2018). The NZ Diploma in Cyber Security aims to provide a pathway for IT graduates or individuals with relevant industry experience to broaden their knowledge and technical expertise through specialised retraining in cybersecurity (NZQA, 2017). Broadcasting, Communications and Digital Media Minister Kris Faafoi (2018) said that the new diploma "will help address the shortage of cyber security professionals". Additionally, to help meet the Cyber Capability goal, the University of Waikato established the Master of Cybersecurity programme, the first master's degree offered in New Zealand.

Scholarships and funding

Generally, private organisations provide most scholarship opportunities in the cybersecurity sector; the only current governmental funding is the GCSB Women in STEM Scholarship. The grant supports female second-year tertiary students and above students studying computer science, cyber security, technology, mathematics, computer engineering, and data science at any New Zealand tertiary institution (GCSB, 2021). GCSB Director-General, Andrew Hampton (2021) expressed that "even if some of the scholarship recipients choose a different career path from the GCSB, we still have an important role in supporting women who are studying STEM subjects". While it is an important initiative to support an equal representation of women in STEM, the scholarship does not go far enough to guarantee further careers in the cybersecurity sector specifically. Under the New Zealand Government's Targeted Training and Apprenticeship Fund (TTAF) announced in 2020, a range of training and apprenticeship programmes at the sub-degree level became free to New Zealand learners. The funding was expanded in 2021 to include the Information technology sector, such as cybersecurity, technical support and web development (Tertiary Education Commission, 2020). Successful privately-funded industry programmes such as the Dev Academy and Summer of Tech have been approved for the TTAF.

Dependence on international talent

The evident challenges that New Zealand faces in training and retaining cybersecurity specialists is reflected in Immigration New Zealand's long-term skill shortage list (NZ Immigration, 2021). Since the New Zealand borders have been closed due to the COVID-19 pandemic since early 2020, the government has worked closely with industry partners to determine the key challenges facing the technology sector. These findings identified a discrepancy between the domestically available skills and what is required for the sector as its greatest shortcoming. To address these capability constraints, the New Zealand Government issued new border exceptions for the technology sector in December 2021

(Clark, 2021):

> We’re carefully targeting areas of the sector where industry has highlighted a clear need for overseas talent including, software development, product managers, cyber security and interactive media. Resolving the skills mismatch is crucial for the tech sector to grow.

Although the government has acknowledged that developing domestic talent is fundamental for the industry to realise its potential, this progress has been painfully slow. In 2019, the Industry Transformation Plan partnership between the Government and the tech industry was established to address the skills and talent pipeline necessary to work in the industry. In addition, progress is underway to develop co-designed Government and industry initiatives to adjust existing qualifications and form a pilot to bridge the work-ready gap. But - as of right now, the extent of this has been largely in research with few outputs (NZ Ministry of Business and Innovation, 2020).

Singapore

Safeguarding Critical Infrastructure

Since the 2000 announcement of the "Infocomm 21 Masterplan", Singaporean officials have sought to develop Singapore into a leading global Infocomm Capital, underpinned by a prosperous digital economy. Accordingly, heavy investments were made in the Internet infrastructure and technology. As a result, cyber-resilient infrastructure reinforced confidence in Singapore as a dependable and trusted international centre for trade and commerce. (Tong, 2000). This ambition was secured into the Intelligent Nation (iN2015) 10-year Masterplan released in 2006, which set Singapore on the path to becoming a global leader in harnessing the Infocomm sector. Emphasis was given to the economic and societal opportunities that ensue from digital connectivity in an increasingly globalised environment while also recognising the potential risks that evolve from cyberspace and highlighting the necessity for these risks to be managed to reap the full benefits of connectivity (Yang, 2006). To this end, Singapore's first Infocomm security master plan (2005-2007) to secure the Government's Infocomm environment, and the second masterplan (2008-2018) that built on its predecessor by expanding inclusion for CII's, were developed to support the iN2015 Secure and Trusted Hub' initiatives. Thereafter, the Infocomm Development Authority launched a five-year

National Cyber Security Master Plan 2018 (NCSM2018) to strengthen existing efforts through three key strategic pillars: enhance security and resilience of CII to deal with sophisticated attacks; increase efforts to promote the adoption of Infocomm security measures among individuals and businesses; and grow Singapore's pool of Infocomm security experts (Infocomm Development Authority, 2013).

The Singaporean government developed commands, programs, and agencies to provide administrative guidance and strengthen the implementation of national cyber masterplans and intelligent nation initiatives. At the 2011 Singapore Global Dialogue, then Deputy Prime Minister Teo Chee Hean announced that Singapore would be setting up a National Cyber Security Center (NCSC) to enhance the government's ability to deter potential cyber-attacks through early detection and prevention. Greater access to cyber information strengthened the government's capacity to respond to potential cyber-attacks and provide more robust protection to critical infrastructure and vital communication systems (AsiaOne, 2011). The NCSC was newly named the Cyber Security Agency (CSA) in 2015 as part of the Prime Minister's Office, acting as the national body overseeing authority on cybersecurity strategy, outreach, education, and industry development. It is administratively overseen by the Ministry of Communication and Information (MCI) (CSA, n.d,a). The Singapore Infocomm Technology Security Authority (SISTA) and National Cybersecurity R & D (NCR) Programme, developed in 2009 and 2013 respectively, were merged into the CSA platform (Ad'ha Aljunied, 2020). The CSA actively regulates and monitors CII sectors; they also support CII owners to help develop their cyber capabilities and build situational awareness. There is an authority from each CII sector that works closely with the CSA. (CSA, 2021a). The Cybercrime Command and National Cybercrime Action Plan (NCAP) established in 2015, and 2016 respectively, function under the Ministry of Home Affairs (MHA). These initiatives work to investigate cybercrimes and plan out necessary priorities to fight against cybercrime in collaboration with the INTERPOL Global Complex for Innovation (IGCI) located in Singapore (CSA, 2016).

The Cybersecurity Act 2018 - a regulatory framework for protecting CII through monitoring and reporting of cybersecurity threats - was passed into Singaporean law on 2 March 2018. The Act defines the designation of CII and the lawful responsibilities of CIIs owners to secure their respective CIIs from the threats of cyber-attacks proactively. Empowerment is given to the Commissioner of Cybersecurity to investigate cybersecurity threats and incidents, utilise the information gathered to ascertain the impact on CIIs and take pre-emptive measures to prevent further harm or future cybersecurity incidents from occurring. It also facilitates critical information sharing by providing a framework for the CSA to request information and share such information (CSA, 2018b). The Cybersecurity Act signified a shift in the approach taken by the Singaporean Government, from the previously perceived notation that cybersecurity was the obligation of individual entities to a nationally regulated sector subject to law. Pursuing a CII focused legislative approach and effectively securitising the sector represents an acknowledgement that disruption of these services can give rise to widespread diplomatic, economic, and societal harm.

Investing in a strong and capable cybersecurity workforce

Youth pathways

Led by CSA, the SC Cyber Youth Programme is a national programme that aims to provide youths with guidance in their cybersecurity journey. Working with academia and industry partners, the programme connects students from the secondary and tertiary sectors by providing access to relevant technical knowledge and opportunities to consider a career in cybersecurity. A key initiative is the Youth Cyber Exploration Programme (YCEP). This cybersecurity boot camp is designed to cultivate excitement among secondary students about their career prospects in cybersecurity, provide education on the fundamental cybersecurity concepts, and offer opportunities to engage in pragmatic assignments and competitions. Since its launch in 2018, in collaboration with five local polytechnics, the programme has trained 700 students from over 30 secondary schools (CSA, n.d,b). In addition, the Cybersecurity Career Mentoring Programme, established in 2017, provides a platform for students to gain invaluable career guidance and support from experienced cybersecurity mentors and industry experts. Other initiatives include the Cybersecurity Learning Journeys and Student Volunteer & Recognition Programme (SVRP). These various programmes are utilised to identify exceptional cybersecurity youth talent, who will be trained under the SG Cyber Olympians programme in advanced cybersecurity skills and international competitions (CSA, 2021a).

Industry-oriented curriculum

Singaporean universities and polytechnics already offer a wide range of cybersecurity programmes for those interested in pursuing an education in cybersecurity, including the Masters in Cybersecurity offered at the Singapore University of Technology and Design

(SUTD). The Singaporean Government has demonstrated a strong commitment to collaborating with Institutes of Higher Learning and industry partners to ensure curriculums and programmes remain relevant to the industry. The CSA is a participating agency in the Ministry of Education's co-operative degree programme to integrate work experience and study (CSA, 2016). Additionally, the CSA works closely with industry partners - companies such as Singtel, Ensign InfoSecurity, and DBS - to provide traineeship opportunities under the SG United Jobs and Skills package to assist new graduates in gaining cybersecurity industry experience (Iswaran, 2020b).

Scholarships and funding

In 2013, Singapore launched the National Cybersecurity R&D (NCR) Programme. Its funding aims to support research projects into human science and technological features of cybersecurity to attract promising individuals in the field and deepen the development of ICT expertise in Singapore. Under NCR funding, the prestigious Scholarship in Cybersecurity is offered to graduate and working professionals looking to further their studies in Cybersecurity, Artificial Intelligence or other Infocomm Media areas (National Research Foundation, 2021).

Mid-career professionals

To advocate for gender diversity in the sector, the SG Cyber Women programme was established to attract more women and mid-year career professionals to pursue a career in cybersecurity. Programmes under the SG Cyber Women include the Ladies in Cyber mentorship programme and technical workshops and Capture-The-Flag for Girls competition (Ann, 2020). Alongside its educational developments, to meet the increasing demand for cybersecurity specialists in Singapore, the CSA facilitates the training of non-cyber security graduates and mid-career professionals for cybersecurity employment roles. Approximately 5,000 Singaporeans have participated in cybersecurity training under the Tech Skills Accelerator programme (Iswaran, 2020c).

Conclusion

While Singapore recognised the significance of cyber threats through its domestic policy approach as early as the 2000s, New Zealand did not begin to respond to cybersecurity until the 2010s politically. Singapore has had more leeway as an illiberal democracy to enable tighter restrictions and limitations to the domestic activity of its citizens in the cyber domain through the enactment of laws, such as the 2018 Cybersecurity Act. Arguably, liberal democracies like New Zealand would find it more challenging to implement a similar approach, given the identity of their country and citizens. The 2013 GCSB reforms make a solid case for this, identifying some of the evident struggles New Zealand face in obtaining security in cyberspace while preserving public faith in the privacy of its people.

Instead, New Zealand has sought to address the concerns of cyber vulnerabilities on critical infrastructure through an array of agencies, systems and frameworks. Initiatives such as the CORTEX system are to be commended for their valuable contributions to securing CII's against cyber threats. However, New Zealand's approach to cybersecurity is arguably fragmented, given the myriad of agencies responsible for dealing with cyber security issues. Netsafe chief executive Martin Cocker says, "the complex web of agencies is needed to address different aspects of cyber security" but agrees there needs to be better coordination of data collection (Bradley, 2021). New Zealand lacks a centralised body of authority in cybersecurity that has been otherwise seen in other small states such as Singapore's CSA. This coordinated approach is reflected in Singapore's educational and outreach efforts to strengthen the pipeline for talent and expertise in the sector. Singapore has adopted a bottom-up approach to securing cyber-security professionals through specialised targeting at different age groups, levels of expertise and gender which the CSA largely oversees. While the New Zealand government has implemented educational opportunities to advance the sector, it remains relatively separate from the industry that informs the necessary skills to do the job. For this reason, New Zealand depends on international talent to fill the evident skill gaps.

Although New Zealand and Singapore share similar attributions as small states, this analysis demonstrates that the countries differ in their approaches to cybersecurity at a domestic level. These differences arguably represent that New Zealand has a greater need for shelter from cyber insecurity than Singapore. This leads into the following chapters that turn this investigation's attention toward examining how and to what degree, are New Zealand and Singapore seek shelter from cyber insecurity through international institutions, regional alliances, and the use of internationally recognised norms and rules.

Chapter Four: The United Nations, International law and cyberspace

Introduction

Given the previously discussed cyber phenomenon's transboundary nature, no country is immune to cyberattacks; these threats do not recognise sovereign boundaries. Without harmonisation of cyber laws, malicious actors continue to exploit jurisdictional gaps between states to their advantage. International cohesion and cooperation are pivotal to collective security due to cyber-activity's scale and transboundary nature. A strong commitment to the UN and multilateral system serves as the bedrock of New Zealand and Singaporean foreign policy. To understand the ways in which New Zealand and Singapore are acquiring shelter from cyber insecurities through international organisations and the use of internationally recognised norms and rules, an analysis of the United Nation's role in cyber governance, norms and laws is imperative.

This chapter seeks to firstly establish the role of small states in the UN, highlighting the importance of the forum to facilitate discourse around cyber cooperation as the only inclusive international forum that affords equal participation to all its members irrespective of size. To this end, a comprehensive analysis of the UN's facilitation of cyber diplomacy will be utilised to demonstrate the history and progress made by the international community to develop a rules-based cyber domain. Developing on this discussion further, New Zealand and Singapore's respective positioning and contributions to the cybersecurity agenda at the UN will be examined.

Small states at the UN

Many small state governments acknowledge that the UN multilateral system works as a great equaliser. Given the vulnerabilities of small states to defend themselves due to their limited resources, as previously discussed, participation at the UN allows small states the opportunity to contribute to global affairs in a manner disproportionate to their size. Embodied in the UN Charter, the UN General Assembly is administered under the doctrine of sovereign equality, otherwise known as one state, one vote, so that all member states are represented and given an equal voice regardless of territorial size, population, or economic capacity. This principle of formal equality among large and small states is a functional mechanism to level the playing field in global affairs (Panke, 2012). Small states can improve their influence in international affairs through cooperation with international and like-minded partners. While compliance by most nations to the international rules-based order is fundamental to global stability and regulating the global commons, there is an essential role that is played by the great powers in this dynamic. There are concerns about the independence of several small states at the UN, considering some have formal and non-formal commitments that compel consultation with larger powers and bear in mind the interests and views of its powerful partners. Owing to small states' reliance on regional and global powers for shelter, some may find themselves subject to influence by larger states (Thorhallsson, 2012). However, in the words of Jim McLay, former New Zealand's UN Permanent Representative, "we know that the alternative to multilateralism is a world where the small can be marginalised" (Súilleabháin, 2014). The UN provides small states with a framework of international laws and treaties that safeguard their sovereignty. Some of the most significant resolutions of the UN, that support the development of multilateralism and global governance originate from major ideas put forth by the UN's small-state members, such as the adopted UN Convention on the Law of the Sea and International Criminal Court (Súilleabháin, 2013). Without the international rule of law, small states would not have the opportunity to have their voices heard on global platforms and participate in international affairs in a way greater than their comparative size. It is not surprising then that small states, such as New Zealand and Singapore, highly value upholding the international rule of law, and extensively advocate for the UN and multilateral system. Many small states share a collective perspective that rules-based multilateralism and its fundamental doctrine of collective security facilitate the very means for its survival. As Singaporean Foreign Minister Vivian Balakrishnan reaffirmed at the 2018 UN General Assembly,

> Compliance with the agreed rules by all states is not only essential for global stability and the governing of the global commons, but is especially important to small states such as Singapore. The principle that agreements will be respected and implemented is fundamental for our survival. Without the rule of law, the strong do what they will, and the weak suffer what they must. Small states like Singapore will not survive in such a world.

Importance of establishing rules and norms in cyberspace

The regime of principles, rules and norms that govern how nation-states should behave are found in virtually all aspects of international political activity such as maritime security (in the form of the UN Convention on the Law of the Sea), trade (with the World Trade Organisation), nuclear weaponry (Non-Proliferation Treaty), or aviation (guided by the rules of the International Civil Aviation Organisation) (Keohane, 2005). As expressed by Singapore's Commissioner for Cybersecurity, David Koh,

> "Cyberspace should not be any different from the physical domain…. Rules underpin our modern economies and our security. Otherwise, the alternative is a world order where might makes right, where rules and norms are routinely flouted, and where there is considerable uncertainty about the sanctity of international agreements and norms. A small state like Singapore is like an ant in a jungle full of elephants, and we must do what we can to better secure ourselves, especially when the elephants fight" (Ghosh, 2019).

To achieve comprehensive cyber resilience, there is a need for accountability coupled with implementing the rules-based international system. To develop a secure, trusted, and open cyberspace underpinned by international law, "it is important that the efforts to discuss such [cyber] laws, rules and norms continue to take place at the UN which is the only universal, inclusive, and multilateral forum, where all States, whether large or small, have a voice" (Balakrishnan, 2018). As the cornerstone of the multilateral system, the UN has a vital role in facilitating global cyber cooperation, particularly in the interests of small states. To this end, a Russian-led initiative concerning the adverse effects of information and communications technologies on the security of states was passed onto the UN agenda during the 1998 UN General Assembly. Since then, the pursuit of establishing global cyber stability has occurred across numerous multilateral frameworks. However, none have been as prominent as the UN Group of Governmental Experts (GGE).

UN and Cyber Diplomacy

Developing cyber norms

The GGE is the central body tasked to advance cooperation and develop stability in the ICT environment and includes the participation of 25 participating states; currently these are Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian

Federation, Singapore, South Africa, Switzerland, UK, US, and Uruguay. Although New Zealand does not directly participate at GGE's discussion, it does actively support dialogue on international cyber law.

While the initial round of meetings in 2004-05 and 2009-10 failed to cultivate crucial progress, the 2012-13 GGE report was groundbreaking. It represented the first time that there was significant consensus by all member states - including the major powers China, Russia, and the US - that international law, specifically the Charter of the United Nations is applicable and necessary to preserving stability and developing an open, secure and peaceful cyberspace. Additionally, it was the first time the great powers agreed and acknowledged that existing international law can be applied to state behaviour in the cyber domain. Political willingness is fundamental in advancing the development and application of norms to state behaviour in cyberspace, especially among the great powers that hold greater diplomatic clout to influence and uphold such agreements.

This progress was further enhanced by the 2014-15 GGE endorsement of 11 informal cyber norms. These new norms sought to guide state activity in cyberspace during the absence of conflict, including the norms that "states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs; states should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure; states should take steps to ensure supply chain security, and should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions; states should not conduct or knowingly support activity to harm the information systems of another state's emergency response teams; states should respect the UN resolutions that are linked to human rights on the internet and to the right to privacy in the digital age" (Rõigas & Minárik, 2015). Thus, progress toward developing universally accepted cyber norms appeared optimistically imminent at that time but was followed by the unsuccessful stalemate of the 2017 UN GGE.

Roadblocks emerge

For the first time since their establishment in 2017, the group failed to reach a consensus on their mandate which is required to release a report. The collapse of the 2017 UN GGE demonstrated the heightened controversy in the cyber domain between the world's great powers, originating from their differing ideological perspectives on how states apply their rights to self-defence, respond to malicious cyber activity, and international humanitarian law

(IHL) (Grisby, 2017). It also reinforced arguments of the cyber revolution thesis, that argued as strategic interests of nation-states become increasingly dependent on cyberspace - such as the economy - there is an opportunity for state actors to exert their influence. This is particularly relevant for the great powers that seek to pursue objectives that threaten the cyberspace of their respective rivals (Maness & Valeriano, 2016).

While the US was fundamentally concerned with constraining cyber conflict through advancing IHL principles of distinction, necessity, and proportionality, Russia and China perceived the standpoint as an attempt to find justification within international law to use cyber mechanisms in the event of a conflict or in response to malicious cyber activity, resulting in destabilising activity (Grisby, 2017). Additionally, the US and their Western allies advocated for a multilateral approach toward developing and furthering international rules and norms in cyberspace based on inclusivity and the free flow of information. However, authoritarian powers, China and Russia, frame information security as a matter of cyber sovereignty. Their primary interests concern the practice of complete state control over digital content to maintain regime stability (Kim, 2014).

The deepening ideological divide illustrates the potential Balkanisation of cyberspace - the emergence of digital borders regulated by global geopolitics - between those who seek to maintain and enforce cyber sovereignty against democratisation and the open free flow of information (Hill, 2012). Divergent perspectives on how international law should be applied to cyberspace activity are particularly concerning small states, such as New Zealand and Singapore, who share an interest in continuing a global order regulated by and subject to international law. As previously discussed, small states do not have the capacity necessary to develop significant offensive capabilities comparable to those of their larger counterparts. The disparity of cyber power between small and large states makes contested debates and gaps in norms extremely concerning (Deibert et al., 2012). In recent years, declining consensus on cyber norms has contributed to global instability in cyberspace, with small states at the frontline of resulting vulnerabilities.

A Way Forward

Despite the 2017 GGE failure, the 2019-2021 GGE was established and successfully achieved consensus to produce a report. The 2021 report is significant given the previous GGE stalemate and it being a time of heightened tensions between key states owing to the frequency and severity of malicious cyber activity targeting fellow GGE members - such as electoral interference and large-scale espionage attacks that occurred during the 2020 SolarWinds incident. This was a major cyber-attack that breached data from multiple parts of the US federal Government and is suspected of being perpetrated by a cyber group backed by the Russian government (Schmitt, 2021). Its remarkable success led to US representative Michele Markoff praising the "political will" of his Russian and Chinese counterparts to "rise above [our] differences" (Markoff, 2021). Of course, achieving consensus did not come without compromise, but the willingness and cooperation of the great powers are to be commended. More broadly speaking, it can be argued that consensus by the great powers represents an acknowledgement that the effects of aggression in the cyber domain are becoming more apparent. Thus, to avoid unnecessary escalation of conflict and preserve their interests, their willingness to cooperate through the establishment of norms is necessary (Forsyth & Pope, 2014).

The recent report's substantive cause for optimism comes from the mutual acknowledgement that IHL applies to cyber operations during an armed conflict, which was previously excluded from the discussion due to objections from China, Russia and Cuba (Efrony, 2021). This has created a basis for discussion to move forward and potentially agree on how IHL governs cyber operations during an armed conflict. On the other hand, minimal progress was made on issues such as sovereignty, due diligence, and countermeasures (Schmitt, 2021). While not groundbreaking in content, the GGE 2021 is to be commended for overcoming the setbacks of the 2017 GGE that did not release a report, achieving consensus despite cyber tensions among member states, and establishing an additional understanding of the 2015 UN GGE norms. Finally, and most importantly, the GGE acknowledged that,

> Continued discussion and exchanges of views by States, collectively at the United Nations on how specific rules and principles of international law apply to the use of ICTs by States is essential for deepening common understandings, avoiding misunderstandings and increasing predictability and stability. Such discussions could be informed and supported by regional and bilateral exchanges of views between States (Schmitt, 2021).

In parallel to the GGE, the UN General assembly established the Open-Ended Working Group on Security of and in the Use of ICTs (OEWG) in 2019 to address the same issues. However, unlike the GGE, this group involves all interested UN member states rather than a set selected number of members - the OEWG includes the participation of all 193 UN member nation-states. Both New Zealand and Singapore are UN member states to contribute to the OEWG. The 2021 OEWG did not contribute substantially to establishing norms of responsible behaviour in cyberspace; instead, it is commended for its successful consensus that represents the first time international security in cyberspace has been an issue discussed by all UN member states (Council on Foreign Relations, 2021). Mainly, the report addressed its commitment to the language and previously established 2015 GGE cyber norms recommendations by many member-states, including voluntary norms and international law. Fellow Josh Gold (2021) claims that “compromise did not come easily, as the OEWG process has been marked by long-standing contention. In the end, no country was fully pleased with the contents of the report”. Although contentious among some states, the report did reaffirm the possibility of future binding obligations in its conclusion (Garvrilović, 2021).

Success in achieving consensus during the OEWG and GGE processes is a reason for optimism about future progress by States to define how international law applies in cyberspace. Consistent commitment to the GGE and OEWG, and other informational forums fosters networking and relationship building for mutual trust. This is a crucial facilitator as the international community seeks to develop collectively recognised norms, or as stated by CSA Chief Executive David Koh (2020), “rules of the road” for responsible State behaviour in cyberspace. By having these important discussions about cyber issues through the UN platform, the GGE and OEWG initiatives allow a range of voices into account, particularly those of small and developing states. Both New Zealand and Singapore have a shared interest in developing a peaceful cyber domain underpinned by the international rules-based order, the maintenance of this arrangement is based on a sense of legitimacy that comes from widespread political support.

New Zealand and Singapore

New Zealand

Internet governance has not historically been at the forefront of New Zealand’s agenda at the UN. Given New Zealand’s expertise and historic commitment to disarmament and role in nuclear non-proliferation treaties, there is a solid argument to be made for utilising its strong background to advocate for international law, norms and regulation in cyberspace (Burton, 2017). New Zealand demonstrates a strong commitment to upholding the international rules-based order through global participation. These values are reflected in New Zealand's Cyber Security Strategy released in 2019, which states,

> "New Zealand's interests will be advanced and protected through our international activity. We will continue to champion a *free, open, secure internet*. New Zealand's voice in international discussions related to cyber issues will support the international rules-based order and promote peace and stability in cyberspace. New Zealand considers that existing international law applies online as it does offline and supports the development and implementation of norms for responsible state behaviour to maintain a peaceful and stable online environment. Cooperation and dialogue on cyber issues is central to building confidence and understanding to reduce the risk of conflict" (New Zealand Government, 2019, p. 13).

Amid the UN GGE and OEWG discussions at the end of 2020, New Zealand released a statement outlining its official position on the application of international law to state behaviour in cyberspace. New Zealand followed several other states that had already done so, including its close partners Australia and the UK. New Zealand's report was critically defining, and significant because it covered contentious issues of international law - such as sovereignty, due diligence, responding to attacks, international humanitarian and human rights law - while also acknowledging that further international discourse is necessary to solidify precise sovereign boundaries in cyberspace and digital specific obligations for due diligence. As a small state with limited global influence outside of international institutions, New Zealand recognises and supports the need for cybersecurity to be addressed through established global forums. New Zealand's perspective on applying international law to state behaviour in cyberspace aligns with upholding the international rules-based order. These norms are interpreted by a Western understanding of the issue that "the openness of the internet is part of its unique value – allowing for unrestricted participation and the free flow of information" (NZ Government, 2019). Taking a similar approach to the US at the 2017 UN GGE, New Zealand agreed that in a time of global cyber conflict, international law would allow the use of defensive cyber means. In New Zealand's 2020 report it was stated that "New Zealand considers that the rule of territorial sovereignty as applied in the cyber context does not prohibit states from taking necessary measures, with minimally destructive effects, to defend against the harmful activity of malicious cyber actors" (NZ Ministry of

Foreign Affairs & Trade, 2020, p.3).

Singapore

As a prominent actor at the frontline of international discourse on cybersecurity, Singapore is considered an international leader in the cybersecurity sector. Enhancing international cooperation to strengthen rules-based multilateralism in cyberspace is the third strategic pillar of Singapore's Cybersecurity Security Strategy (2021). It outlines that,

> As a small state, Singapore firmly supports the establishment of a rules-based multilateral order. Developing and implementing voluntary and non-binding norms are important steps toward this objective. We must help develop and abide by rules that all States agree to follow, which in turn guide responsible State behaviour in cyberspace.

Singapore has strategically leveraged its membership at the UN to bring attention to cybersecurity. During the 2018 UN General Assembly, Singapore's Foreign Minister, Vivian Balkrishnan took the opportunity to advocate for the development of rules and norms to govern cyberspace,

> "We urgently need to promote the adoption and implementation of rules and norms in cyberspace. To reap the full benefits of digital technologies, we must develop a trusted and open cyberspace underpinned by international law and well-defined norms of responsible State behaviour. As the only universal, inclusive, multilateral forums, States have always turned to the UN to develop the rules that govern the global commons. One example is the UN Convention on the Law of the Sea (UNCLOS), which provides the global legal framework for all activities in the oceans and seas" (Balkrishnan, 2018).

Singapore actively participates and contributes to international discussions on cybersecurity, such as the UN GGE where the nation is one of 25 members. Its participation in these platforms has been an opportunity for Singapore to advocate for international law - particularly the UN Charter - and how it applies to state behaviour in cyberspace and emphasise the essentiality of State's adherence to the cyber normative and stability framework (UN, 2019). As a GGE member in 2021, Singapore contributed its national position on applying international law in cyberspace to the UN. It clarified Singapore's perspective on state activity that can and cannot be taken in cyberspace to strengthen the international rules-based order. This position reaffirmed US-led views on self-defence and international humanitarian law by asserting: “a State has the inherent right of self-defence if malicious cyber activity amounting to an armed attack, or an imminent threat thereof, occurs against that State; and Singapore’s view is that in times of armed conflict, the relevant principles of international humanitarian law (“IHL”) would apply to the belligerents’ use of cyberspace. Some examples of such principles would include those of humanity, necessity, proportionality and distinction” (Cyber Law Toolkit, 2021). While Singapore has adopted its own domestic laws to regulate free speech and has refrained from terminology associating cyberspace with the free flow of information, it appears that its interests are informed by the historical Western perspective when it comes to the international arena. To support the facilitation of discussions going forward, Singapore will be chairing the OEWG 2021-2025.

Additionally, Singapore co-chairs the UN Group of Friends on Digital Technologies and co-chairs the UN Group of Friends on e-governance and cybersecurity (Ministry of Foreign Affairs Singapore, 2022). In October 2020, Singapore strengthened its collaboration with the UN to build cyber capability by announcing the development of a norms implementation checklist. This checklist encourages the adoption of the 11 voluntary, non-binding norms for responsible behaviour in cyberspace outlined in the 2015 UNGGE consensus report. By considering diverse national interests and capabilities, the checklist is critically refined to be applicable to a range of UN members. UN Under-Secretary-General and High Representative for Disarmament Affairs Izumi Nakamitsu emphasised the importance of the checklist to help countries move forward from statements of principles to the adoption of more practical and tangible steps of implementation (Iswaran, 2020a).

Conclusion

International organisations provide a substantial level of shelter that is arguably more acute for small states like New Zealand and Singapore. At the centre of the international-rules based order, the multilateral nature of UN platforms affords small states security otherwise unattainable through greater representation and contribution to global affairs alongside its larger counterparts. Compliance with the agreed-upon rules and norms is security enabling, and while common behaviour is in the interests of all states, it is particularly imperative to the survival of small states.

In the absence of global regulation on state activity in the cyber domain, the GGE and the proceeding development of the OEWG are to be commended for bringing cybersecurity to the forefront of discussion among the international community. It has allowed the interests and perspectives of all states – big and small - to be considered in the efforts to cultivate norms and rules in the cyber domain. The platforms have also provided the great powers with a neutral forum to consider and discuss their ideological grievances in cyberspace to overcome the barriers that currently limit consensus. While it is demonstrated that these forums have made remarkable progress in cultivating international discourse on cybersecurity, it is important to keep in mind that consensus on a matter of rules and norms does not directly translate into implementation in the absence of binding regulation. Despite this, efforts such as consensus at the 2014-15 GGE to endorse 11 informal cyber norms are significant in establishing a common baseline to which countries can hold each other accountable. Furthermore, a shared understanding of acceptable state practices in cyberspace allows the international community to intervene with critique and diplomatic pressure if states choose to ignore these norms in their activity.

By having these discussions at the UN, New Zealand and Singapore have acquired shelter through their participation and contributions to the international cyber agenda. Releasing official statements on the application of international law in cyberspace have allowed the interests of New Zealand and Singapore in the cyber domain to be reflected at the UN. These statements are meaningful contributions to the ongoing development of customary international law in cyberspace, pivotal to building confidence and shared understanding that diminishes the risks of conflict. Especially when you consider there remains contested debate as to how international law applies to state activity in cyberspace between the great powers. New Zealand and Singapore's involvement in the international discourse on cybersecurity issues will reinforce the importance of uploading the international rules-based order in cyberspace.

Although the international community may seem far away from adopting an agreed-upon treaty or governance framework to regulate state behaviour in cyberspace, as history suggests, there is potential for current efforts to evolve into an enforceable agreement. This was seen during the development of the Treaty on the Non-Proliferation of Nuclear Weapons. States began acquiring nuclear weapons as early as the 1930s, but addressing non-nuclear proliferation did not reach the UN agenda until a US-led proposal was presented to the UN

General Assembly in 1953. Negotiations that ultimately led to the formal signing of the first international treaty to prevent the spread of nuclear weapons in 1968 were an extensive process (UN, 2015). As the GGE and OWEG discussions proceed, there are evident hurdles to overcome. However, despite these challenges, state actors continue to demonstrate a desire and willingness to progress these issues at the UN. Arguably, regional organisations have provided a more substantive platform for many small states to seek shelter from cyber insecurity. In the following chapters, the most prominent regional platforms to both New Zealand and Singapore will be explored at length to show this.

Chapter Five: New Zealand and the Five Eyes Network

Introduction

New Zealand is a member of the Five Eyes (FVEY) – a multilateral intelligence-sharing arrangement with the Anglosphere – that dates back to the Second World War era. The partnership is central to New Zealand's approach to security and intelligence. Owing to the limited size of New Zealand's intelligence agencies, the FVEY network affords greater intelligence, technology and support than otherwise attainable. In the contemporary security environment, balancing strong security ties with its traditional Anglosphere partners while maturing its economic relationship with China is New Zealand's greatest foreign policy challenge. Maintaining this balancing act is strongly in the interests of New Zealand, particularly in the preservation of its cyber interests with the FVEYs. This chapter explores how New Zealand, as a small state, has acquired shelter from cyber insecurity through its membership with the FVEY network. It begins with a brief historical overview of the FVEY network's development, operational and cultural nature. This is followed by providing an extensive overview of the significance of the FVEY arrangement to New Zealand's ability to produce the necessary security and intelligence that serves its national interests. Expanding on this, an examination of New Zealand's other intelligence arrangements with FVEY partners is explored. Lastly, this analysis concludes with a discussion of New Zealand's dilemma in balancing its interests with the FVEY network and economic powerhouse, China. Moreover, it considers the ways in which New Zealand is preserving its independent foreign policy to maintain the balancing act.

FVEY Background

New Zealand, Australia, Canada, the United Kingdom (UK), and the United States (US) are the FVEY intelligence community members, the world's most enduring and exclusive intelligence network. Originating from the United Kingdom – United States of America Agreement (UKUSA) of 1946, New Zealand, Australia, and Canada were explicitly named "UKUSA-collaborating Commonwealth countries" when the agreement was updated in 1955 (Cullen & Reddy, 2016). While no official overarching global agreement governs the FVEY intelligence partnership, the links that bind the members together are more robust than might seem the case at first glance, given their far-flung geographies (Cox, 2012).

The term 'Anglosphere' is often used to group these five nation-states, unified by their deep historical and cultural ties to the traditional common law of the Great British Empire (Wellings & Mycock, 2019). United by shared liberal institutional frameworks, the FVEY partners' prosperity is based upon common principles of liberal democratic values, language, and complementary national interests (Hulsman, 2020). Since the late 20th century, the Anglosphere has acted as a bedrock to "define, order and promote" the values, policies and multilateral institutions that underpin the liberal international rules-based order (Vucetic, 2010). However, in the contemporary security environment, the FVEY network is bound by more than their shared history; specifically, the challenges posed to them from similar national security threats, conventional and unconventional. The extent of cohesion shared between the FVEY partners is illustrated by their disclosed commitment not to target the intelligence agencies or citizens of each other. While there is no formal approach to ensure spying does not occur, the members share mutual trust that each adheres to this 'gentleman's agreement' (Cox, 2012).

Strategic importance to New Zealand security

Over time, the FVEY partnership has become more important and integral to New Zealand. GCSB Director-General, Andrew Hampton, and Director-General of Security, NZSIS, Rebecca Kitteridge, have acknowledged that,

> International intelligence-sharing arrangements are fundamental to how GCSB and NZSIS meet New Zealand’s national interests. New Zealand could not hope to deliver the current level of security and intelligence activity alone. Our most significant relationship is with the Five Eyes partnership. The Five Eyes partnership has been central to New Zealand’s approach to intelligence and security since World War II…We could not do our job without the support we receive from our Five Eyes partners (NZ Government, 2017).

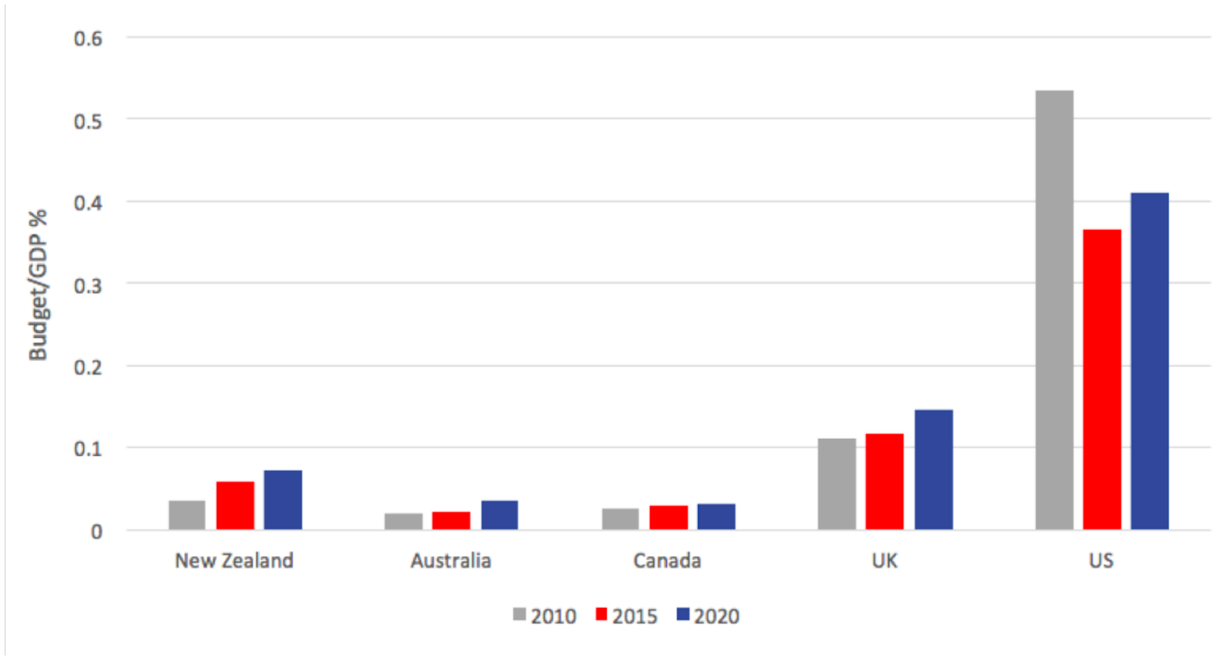
Given that national security threats stemming from the cyber domain are becoming more transnational and complex in nature, it would be very costly for New Zealand to establish its own self-reliant intelligence capability. This is compounded by New Zealand’s relatively smaller size and material capabilities compared to their FVEY partners. The GCSB website on the UKUSA partnership emphasises that “it is not possible for an organization the size of the GCSB to collect intelligence on all threats to New Zealand’s national security interests.

However, through New Zealand's long-standing partnerships, we can draw on greater support, technology and intelligence than would otherwise be available to us" (GCSB, 2022).

Each member of the FVEY network "collects information over a specific area of the globe in accordance with their national priorities, but their collection and analysis activities are orchestrated to the point that they essentially act as one" (Cox, 2012). While exact areas covered are not publicly acknowledged, research suggests that Australia covers South and East Asia; the UK commits its resources to Europe and Western Russia; the US monitors China, Russia, and the Middle East; lastly, New Zealand covers the South Pacific and Southeast Asia (Gee & Patman, 2021). Owing to its unique geographical location, New Zealand can monitor signals from approximately a quarter of global geostationary commercial satellites (Cullen & Reddy, 2016). Through the FVEY partnership, New Zealand has access to a greater information pool, technology capabilities, and skills than would otherwise be attainable on its own. Additionally, the extensive nature of the FVEY network and its other foreign partners allow New Zealand to focus and prioritize its intelligence gathering and assessment resources on its immediate region and on operations that are of most importance to it, in alignment with its national interests, while averting intelligence gaps. (Cullen & Reddy, 2016).

Figure 1

National Intelligence Budgeting of Five Eye member states 2010-2020



Note. Values are given in USD. Data sourced for New Zealand from New Zealand Treasury, for Australia from Australian Department of Foreign Affairs and Trade, for Canada from Treasury Board of Canada, for the UK from Government Digital Service, for the US from Office of the Director of National Intelligence.

Figure 2

National Intelligence Budgeting of Five Eye member states 2010-2020

	New Zealand	Australia	Canada	UK	US
2020/21	155m	475m	521m	3.98b	85.8b
2015/16	100m	302m	460m	3.4b	66.8b
2010/11	52m	217m	404m	2.7b	80.1b

Note. Values are given in USD. Data sourced for New Zealand from New Zealand Treasury; for Australia from Australian Department of Foreign Affairs and Trade, for Canada from Treasury Board of Canada, for the UK from Government Digital Service; for the US from Office of the Director of National Intelligence.

Like Australia and Canada, New Zealand's participation in the FVEY network is unequivocal as a junior partner to its larger counterparts - the US and the UK - where the exchange of intelligence and information is generally one-way (O'Neil, 2017); what New Zealand gains from the network are far greater than what it contributes. For every intelligence report the GCSB makes available to its partners, they receive access to 99 international reports in return (Cullen & Reddy, 2016). Occasionally, partners put forward requests to the GCSB for intelligence collection assistance. However, due to limited capabilities and capacity constraints at the bureau, very few submitted requests are completed (Cullen & Reddy, 2016). As such, 'requests are only fulfilled where they align with New Zealand's intelligence-gathering priorities and fall within the GCSB's statutory mandate' (Cullen & Reddy, 2016). As shown in Figure 1 and Figure 2, New Zealand is the smallest economy of all five countries in the network, with a significantly smaller national budget for intelligence than larger partners. For example, New Zealand's 2020/21 intelligence community budget totalled USD 155m, whereas the US budget is approximately 550 times this amount standing at USD 85.8b (NZ Treasury, 2020; Office of the Director of National Intelligence, n.d).

New Zealand's membership in the FVEY network is an integral part of its national cyber security strategy. For example, the aforementioned CORTEX initiative - New Zealand's central suite for advanced cyber defence capabilities - is designed to leverage the distinctive capabilities granted to New Zealand as a member of the FVEY network. Speaking about the role of the FVEYs in the development of the CORTEX suite at the Aspen Institute Cyber

Summit Forum in early November 2018, Hampton stated that (2018),

> We took a range of standard products and combined them with the unique cyber threat insights available to us through our Five Eyes relationships. This allows us to deliver cyber threat detection and disruption capabilities typically not available through commercial providers. We also contribute unique insights to our Five Eyes partners about the malicious activity we are seeing on New Zealand networks.

Cooperation among the partners on intelligence does not mean that the five states pursue a collective foreign policy approach. As a small state, New Zealand has benefited from the multilateral nature of the FVEY partnership, which has provided shelter during disputes with other members (Brunatti, 2016). Notably, when US-NZ relations deteriorated at the end of the 1980s and Washington suspended its obligations to New Zealand under Australia, New Zealand, United States (ANZUS) Security Treaty, the other members of the FVEY network encouraged the US to show restraint. British Intelligence Coordinator, Sir Antony Duff, lobbied for New Zealand in Washington and emphasized that “Mrs Thatcher herself had stressed to President Reagan the importance of maintaining New Zealand’s intelligence flow” (Hensley, 2006). Although not in agreement with New Zealand’s anti-nuclear legislation, the Australians reaffirmed their intelligence cooperation with Wellington and in a memorandum to the Australian Cabinet reported that “it is in our interest that New Zealand’s isolation from the broader Western intelligence community be minimized” (Cabinet Minute, 1985). It was later acknowledged by the US National Security Agency (2007) that,

> Most of us remember when the New Zealand government forbade port calls by ships carrying nuclear weapons in 1985. When the government stood firm, many U.S. contacts at all government levels were halted or curtailed. On the SIGNIT side, *the policy did not splinter our relationship*.

Continued cooperation between the FVEY SIGNIT intelligence organisations after the US-New Zealand crisis in the 1980s meant that New Zealand did not have to confront the high costs involved in creating an autonomous intelligence capability. Further, the strong and independent stance that New Zealand took on nuclear security demonstrates how New Zealand’s membership in the FVEY network has not limited its ability to have an independent foreign policy on specific issues. In practice, the Five Eyes network is ‘more of a cooperative, complex network of linked autonomous intelligence agencies’ (Cox, 2012) rather than a centralised body. The intelligence agencies of each member state act in accordance with their own legislated mandates and operate within their own complex legal frameworks. Individual intelligence organisations of the partnering states,

> interact with an affinity strengthened by their common Anglo-Saxon culture, accepted liberal democratic values and complementary national interests, all seasoned with a profound sense of confidence in each other and a degree of professional trust so strong as to be unique in the world (Cox, 2012).

Cooperating on intelligence outside of FVEYs

As a member of the FVEY network, New Zealand has benefited from closer cooperation in other areas. In January 2013, the New Zealand government announced a deal with the UK government that would allow New Zealand to reap the benefits of cyber-related research and development activities at a new international cyber security facility in the UK (GCSB, 2013). In November 2018, New Zealand and Australia established the Pacific Cyber Cooperation to closely work with the Pacific Islands and enhance the cyber resilience of the region (Peters, 2018). In addition, New Zealand is an active member of the annual Five Country Ministerial (FCM) meeting on home affairs, public safety, interior, security, border and immigration with Australia, Canada, the UK and the US that commenced in 2013. The FCM is separate from the FVEY network that focuses on shared national security issues and concerns, covering a broad range of topics from counter-terrorism and aviation security to countering child exploitation and online harm (Department of the Prime Minister and Cabinet, 2021). At the 2018 FCM, the attorneys-general from each participating state attended to discuss “emerging issues and collaboration in countering foreign interference, the challenges posed by ubiquitous encryption, criminal information sharing and addressing the financing of transnational crime and terrorism” (Australian Department of Home Affairs, 2020). The discussion resulted in a commitment by all member states to establish a mechanism to share developments on each country’s respective approach to tackling the threat of foreign interference and “in the event of a severe foreign interference incident within our sovereign nations, we agreed the five countries would coordinate on appropriate responses and attribution” (Australian Department of Home Affairs, 2020). This commitment was realised in September 2020 when New Zealand signed the Antitrust Cooperation Framework with its

FVEY partners to permit the sharing of confidential information and compulsory processes for investigative assistance to counterparts (Federal Trade Commission, 2020).

Five Eyes and China: New Zealand's dilemma

Like many small states, New Zealand is at a pivotal point as it navigates the complexities of the contemporary security environment – out of the shifting balance of power, a new global order is arguably emerging. While all states must manage the potential dilemmas that arise, small states reliant on the protection of great powers for their security and open international trade for economic prosperity are distinctly vulnerable. Historically, New Zealand's colonial history and foreign policy interests have drawn the government closer to alliances and alignments with its traditional partners, the UK, the US, and Australia. While New Zealand's robust security relationships remain with the Anglosphere, it has established a strong and prosperous economic partnership with China's emerging global economic powerhouse (Brady, 2019). Since 2017, China has been New Zealand's largest trading partner, and by 2019 it accounted for $33b of New Zealand's trade and 30% of its exports (NZ Ministry of Foreign Affairs, 2019). As such, the continued economic prosperity of New Zealand has been closely linked to a perceived dependency on China. In the past, New Zealand could rely on shared values, a common culture and security, military and intelligence cooperation to smooth interactions with the US and UK. Still, New Zealand does not have this with China (Steff & Dodd-Parr, 2019). Instead, the model for the New Zealand-China relationship is based on "seeking common points; facing up to differences" (Brady, 2008, p.1). Since the early 2010s, New Zealand's foreign policy approach has focused on maintaining a balancing act to preserve strong security ties with its traditional partners, particularly the US and Australia, while maturing its flourishing economic relationship with China in a way that does not impinge upon New Zealand's relations with the former. Managing the relationship with China requires the New Zealand government to consider balancing its economic interests against its sovereignty and national security. Facing a time of global uncertainty and mounting geopolitical competition, balancing relations with opposing great powers has become more complex; getting the relationship with China – and the US - right is arguably the greatest challenge facing New Zealand foreign policy.

New Zealand's balancing act with its traditional FVEY partners and China has sparked a debate. Some claim that New Zealand has become the weakest link among the FVEY owing to its extensive political and economic exposure to Chinese influence. Anne-Marie Brady, a specialist in Chinese politics, has concluded that "In New Zealand, reference to foreign interference almost always relates to the foreign interference activities of the CCP government" (Brady, 2021, p. 71). These efforts have granted Beijing access to the political core of New Zealand. For example, in 2017, it was revealed that former New Zealand politician Yang Jian had concealed his fifteen years working in China's military intelligence sector and Chinese Communist Party (CCP) membership. During his tenure in parliament, Yang played an influential role in shaping the New Zealand National government's strategy with China, promoting engagement with the New Zealand Chinese community and facilitating fundraising efforts among the Chinese community. In his position alongside former New Zealand Prime Minister John Key, Yang was granted privileged access to New Zealand's China policy briefing notes and positions during diplomatic visits to China and meetings with senior officials (Brady, 2017). In recent years, New Zealand has received increasing criticism from the media in FVEY nations, from some academics and the odd FVEY politician for being 'soft on China' and prioritising New Zealand's economic interests; as such, Wellington has allegedly taken a cautious approach when it comes to matters that violate the values of the international rules-based order (Köllner, 2021; Brady, 2019; Coughlin, 2021; 60 Minutes Australia, 2021). Anne-Marie Brady has concluded that New Zealand is valuable to China as the soft underbelly to access Five Eyes intelligence (Brady, 2018). Christopher Johnson from the Center for Strategic and International Studies in Washington has warned that New Zealand may present as a softer target to Beijing in comparison to its larger counterparts and thus "it may also be using it as a testing ground for future operations in other countries" (Angerlini, 2017). This has prompted the FVEY's to informally expand its intelligence-sharing remit, specifically around classified information on China, with other like-minded nations such as Japan and Germany that have similar concerns (Barkin, 2018).

Maintaining New Zealand's independent reputation

New Zealand's security and intelligence agencies have demonstrated their mindfulness toward potential cyber security threats originating from China. In December 2018, the GCSB blocked Huawei's involvement in New Zealand's 5G network development, citing significant national security risks. The telecommunications company is closely linked to the Chinese Ministry of State Security and has been actively involved in attempting to shape public opinion in New Zealand (Keall, 2018). It is a significant advertiser in multiple New Zealand media organisations, including NZME, New Zealand Herald and Stuff, as well as a sponsor for New Zealand universities and think tanks (Sin, 2017). Additionally, Huawei's historical allegations of copyright violations and intellectual property theft, coupled with its links to Chinese intelligence authorities, have created fears for its involvement in developing and upgrading 5G network technology. Although company officials have denied its relationship with the CCP, it is apparent that Huawei is obligated under law to cooperate with Chinese state intelligence agencies (Yang, 2019). Nonetheless, Andrew Little emphasised that barring Huawei from the 5G network development was due to a technological risk assessment rather than the company's affiliation with the Chinese government (The Strait Times, 2018). Given New Zealand's attempts to minimise public disagreement with China over the years, the Huawei ordeal is unique. It reflects a fundamental divide between Wellington's democratic worldview and the assertive nature of China's centric. Between February to December 2019, the first inquiry into foreign interference in New Zealand was held by parliament. While officials and politicians refrained from naming China in discussions, it was evident that the inquiry intended to investigate the covert actions of the CCP government. Various vectors for foreign interference were explored, including 1) cyber-enabled threats, 2) the use of traditional and social media to disperse influential misinformation and 3) building covert influence and leverage over political officials (Kitteridge, 2019). Changes followed this in several domestic laws and the signing of the aforementioned anti-trust investigations cooperation agreement with FVEY partners. In July 2021, Minister for the GCSB and NZSIS, Andrew Little, issued a statement titled New Zealand condemns malicious cyber activity by Chinese state-sponsored actors that specifically called out the Chinese Ministry of State Security (MSS) for its malicious cyber activity both in New Zealand and globally (Little, 2021). The timing of its release was coordinated with the other FVEY members, the EU, NATO, and Japan, which represents a potential argument for small states being involved in the collective attribution of cyber incidents for security. Additionally, the use of unusually direct language leaves no scope for reinterpretation by explicitly identifying "Chinese state-sponsored actors" as the perpetrators of the early 2021 Microsoft Exchange cyber-attacks - directly relating the threat to New Zealand. The firm nature of the statement is perhaps a diplomatic signal to both China and New Zealand's Western allies that when it wants to, "New Zealand can talk tough on China" (Miller, 2021). New Zealand's willingness to speak out on malicious state activity in cyberspace is informed by its national interests and values as outlined in New Zealand’s Cyber Security Strategy (2019),

> We will act bilaterally, regionally and globally to build trust in cyberspace. We will respond to unacceptable behaviour in cyberspace and we will cooperate with others to prevent and deter malicious activity that threatens peace and security.

As a key domain of contemporary international relations, the cyber realm is a prominent area of importance for the FVEY arrangement. As such, there is no doubt that members of the network will support the outspoken nature of New Zealand’s statement. Furthermore, suppose New Zealand had not publicly expressed explicit criticism of China’s cyber activities. In that case, it may have led to growing concerns over New Zealand’s independent foreign policy from its FVEY partners. In other words, a small state like New Zealand, despite its independent credentials, still needs to consider the interests – and views – of its partners.

Conclusion

In the historical and contemporary security environment, it is evident that the FVEY arrangement remains integral to New Zealand's cybersecurity approach. New Zealand's participation in the FVEY network is as a junior partner; what New Zealand gains from the partnership is much greater than it contributes. New Zealand could not hope to achieve its current level of security and acquire as much intelligence without this arrangement, given its inherent structural weaknesses. If New Zealand did not have access to the highest-quality intelligence and research capabilities granted to them by its more powerful partners, it would be forced to outlay more expenses on protecting its national security. This would be difficult to attain owing to its relatively small size and limited resources. By having access to widespread global information from its like-minded partners, New Zealand has greater clout to contribute towards the formulation of its foreign policy decisions, including those related to cyber issues.

New Zealand's balancing act to maintain its security ties with traditional FVEY partners and mature its flourishing economic relationship with China has introduced new complex issues to foreign-policy makers. In a time of global uncertainty and increasing geopolitical competition, New Zealand's exposure to Chinese political influence has sparked a new debate about New Zealand's position with the FVEYs. Professor Anna-Marie Brady has gone as far as to label New Zealand as the soft underbelly for the Chinese government to infiltrate FVEY international security and intelligence. In this context, New Zealand security agencies have demonstrated their mindfulness of Chinese cyber threats through its governmental decisions to block Huawei's development of 5G technology, national enquiries into foreign interference and standing up against unacceptable behaviour in cyberspace. New Zealand's strong stance on China in the cyber domain supports efforts to preserve its independent foreign policy in the FVEY arrangement. The next chapter investigates Singapore's most significant regional arrangement with ASEAN.

Chapter Six: ASEAN Cybersecurity and Singapore

Introduction

In the contemporary landscape, the Association of Southeast Asian Nations (ASEAN) provides Singapore with an amalgamation of economic and political shelter by dealing with traditional and non-traditional security issues. ASEAN forums allow Singapore to have a voice in regional and international discussions on security challenges that directly relate to its own strategic interests and survival. In recent years, the ASEAN grouping has given increasing attention to the relevance of the cyber domain as a critical facilitator of economic progress. In recognition of the direct links between the security of the economic environment and the challenges of an evolving cyber domain fraught with new threats, cybersecurity has become a significant focus of the ASEAN agenda. In this context, Singapore has played a key role in enabling progress on cybersecurity within the ASEAN grouping and among its wider international partners.

This chapter seeks to provide a comprehensive analysis of ASEAN's approach to cultivating cooperation in the cyber domain to determine how these efforts provide shelter to Singapore. It starts with an overview of Singapore's historical relationship with ASEAN, highlighting the strategic importance of ASEAN in Singapore's foreign policy. This is followed by examining how Singapore's national interests as a Smart Nation are intertwined with the well-being of the ASEAN cyber landscape. The chapter then outlines how ASEAN is making progress in the cybersecurity sector, with a distinct focus on how these efforts are aligned with Singapore's interests in the sector. Finally, it concludes with an analysis of Singapore's contributions to ASEAN's cybersecurity agenda and how the small-city nation has leveraged its position as an influential leader within the regional grouping to shape this approach and in doing so, acquiring shelter.

Background of ASEAN

ASEAN consists of Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Singapore was one of the five original signatories of the ASEAN Declaration upon its establishment in 1967. At the time, ASEAN nations were among the most impoverished in the world; now, ASEAN is the fifth largest global economy with a regional GDP of USD$3.08 trillion and home to 679 million people (Hawksford, 2017; O'Neill, 2021). Since its inception, ASEAN has become a powerful diplomatic platform to foster regional stability and extend its interests to economic and social integration. To defend against the challenges of globalisation and economic growth of its member states, ASEAN leaders recognised that it needed a clearly articulated identity that represented a sense of "common destiny". In recognition of this, ASEAN adopted the motto "One Vision, One Identity, One Community" (Mathews & Pereira, 2020).

Importance of ASEAN to Singapore

Since Singapore became an independent state in 1965, the small city-state has had to be strategically pragmatic in its approach to political and economic policies. Without any natural resources and hinterland, Singapore's survival and prosperity have been closely linked to successfully leveraging external opportunities and resources. Singapore is to be commended for transforming from a Third World to a First World country in only 50 years despite the limitations of its size and vulnerabilities. In this backdrop, ASEAN has played an essential and strategic role in shaping an external environment for Singapore to succeed in its domestic transformation (Lim, 2017). While the character, perceptions, and importance of Singapore's membership in ASEAN have developed over the years, its membership has remained a prominent pillar of Singapore's foreign policy and broader economic strategy. The Singaporean Government seeks active and cooperative membership within ASEAN to achieve and enhance the state's security, global positioning, economic growth, and competitiveness. The strength of the regional platform is key to Singapore's engagement with regional and international partners.

The ASEAN economy is one of the fastest-growing economies worldwide, driven by a commitment to free, open trade and regional integration through the rules-based multilateral trading system. The ASEAN Free Trade Agreement (AFTA) opened several strategic pathways for Singaporean companies to trade freely with other ASEAN countries. Under the ASEAN Economic Community (AEC), the ambition to integrate the ten economies into a single market and production base will widely boost ASEAN's capacity toward becoming a global economic powerhouse. Collaborating through the AEC, it is projected that ASEAN will become a borderless economic digital community by 2030 (Hawksford, 2020). This means Singapore's domestic market would amplify from its populated 6.45 million consumers to 679 million. Singapore has been a regional signatory to the formation of 10 regional free trade agreements, including ASEAN-China, ASEAN-Australia-New Zealand, ASEAN-Korea Free Trade Area and ASEAN-India. Trade agreements with these countries reduce over 90% of all tariffs and shape an attractive perspective of ASEAN states to international business partners (VietnamNet, 2015). Additionally, Singapore has signed two internationally significant FTAs, notably the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the European Union-Singapore Free Trade Agreement (EUSFTA) (Hawksford, 2020).

ASEAN incorporates an open and inclusive attitude to develop friendly international partnerships and mutually beneficial dialogue. ASEAN Dialogue partners include Australia, Canada, China, the European Union (EU), India, Japan, New Zealand, Korea, Russia, the US and the UK. ASEAN state leaders and the leaders of its dialogue partners meet annually to participate in ASEAN-led forums such as the ASEAN Regional Forum, East Asia Summit (EAS) and ASEAN Plus Three (China, Japan and South Korea). By providing ASEAN leaders with a platform to connect with leaders from the world's most prominent countries, member states are given increased exposure to engage in discussions surrounding regional security issues and strengthen their cooperation and collaboration with participants (Koh, 2018). Arguably, annual platforms to collaborate with international partners on a range of international affairs would otherwise be unattainable for small states like Singapore without ASEAN. In the words of Singapore's former permanent representative to the UN, Tommy Koh (2018) "Without ASEAN, none of the 10 member states would be able to attract the leaders of the most important countries of the world to meet annually with them".

ASEAN Cybersecurity and Singapore's Smart Nation strategy

Singapore - located at the juncture of the Strait of Malacca - is a maritime, banking and aviation hub where a significant portion of global capital and freight travels. The nation has been acknowledged for its economic stability and corporate-friendly environment, perfectly placed as a strategic gateway to Southeast Asia and the wider Asia Pacific region. As Singapore continues its ambitious Smart Nation initiative previously discussed in Chapter Two and integration into a borderless AEC, the nation must consider how its economic growth and prosperity are closely linked to the well-being of the ASEAN region. If the region can manage cyber risks and threats, it can reap the full benefits of digitalisation (Ponti, 2021).

Speaking about Singapore's leadership on ASEAN cybersecurity, David Koh (2021), Chief Executive of the CSA conceded,

> No man is an island, all more so in cyber issues. The nature of digital is cross border international. The country must realise that no matter what happens in Singapore, it would not be sufficient to curtail the widespread cyber threats. Singapore knows that its economic growth is tied to the ASEAN region thus building up the region's cyber resiliency is vital.

Owing to the increasing strategic relevance and digitalization of the region, ASEAN members are becoming prime targets for cyber attacks. While some states have made significant progress in securitizing their digital landscape, cyber resilience across the region remains low. This is largely owing to disparities among member-states in cyber capabilities, governance and policy. Consequently, ASEAN countries are being used as springboards for cyberattacks, presenting as either vulnerable CII's that are easily accessible for large-scale attacks or hubs that only require a singular point of attack to obtain access to its wider international connections (Chua & Dobberstein, 2020). At the 5th ASEAN Ministerial Conference on Cybersecurity (AMCC), Minister S Iswaran (2020b) warned,

> Many cities within ASEAN serve as key hubs for services spanning the banking and finance, telecommunications, aviation and maritime sections. Thus, the impact of a cyberattack on a national CII may not be confined to that country alone, but also felt in other parts of the region, and even the world.

Recognising that cyber threats do not respect sovereign boundaries and that cyberattacks can exploit jurisdictional gaps between nations, Singapore acknowledges strengthening international partnerships, especially among ASEAN members, to address transnational cybersecurity issues as one of the three strategic pillars of the 2021 Cybersecurity Strategy (CSA, 2021a).

ASEAN Digital Economy

ASEAN is at the centre of the world's fastest-growing internet region. In 2014, ICT investment amounted to approximately USD$100 billion, and it is estimated that by 2025 digital spending could raise more than US$200 billion in the region (Hawksford, 2020; Ponti, 2021). As the fastest-growing global economic region, the resilience of cyber economic technology has become a prominent factor in its future prosperity. ASEAN's strong and flourishing economy, ICT investments and ongoing economic integration underpin the region's potential to become a global leader in the digital economy (Chua & Dobberstein, 2020). By 2025, ASEAN's digital economy has the potential to contribute $1 trillion to its GDP (Ramadhan, 2020). Achieving this economic ambition requires all ASEAN member states' shared effort and vision.

The ambition for digital acceleration is reflected in the ASEAN Digital Masterplan 2025 (and previous versions) that seeks to propel "ASEAN as a leading digital community and economic bloc, powered by secure and transformative digital services, technologies, and ecosystem". The report outlines three key areas for enhancing regional cooperation: developing innovative ICT infrastructure, inclusive talent ecosystem cultivation, and green and sustainable development (CIO, 2021).

However, failing to respond to the risks and challenges posed by cyber threats will undoubtedly impede the resilience of the digital economy, undermine the proper functioning of markets and withhold the region from recognising its full economic potential. ASEAN's commitment to regional cybersecurity is heavily founded upon recognition by member states that for the digital economy to flourish both domestically and internationally, the digital economy of each member state needs to be secure. At the 13th East Asia Summit held on 15 November 18, ASEAN member states and participating international partners (Australia, China, India, Japan, Korea, New Zealand, Russia and the US) acknowledged,

> “the vital importance of information and communications technology (ICT) security for the digital economy, given that an open, secure, stable, accessible, and peaceful ICT environment is critical to connectivity and the economic development of the EAS participating countries, as well as the digital economy’s increasingly important role as a driver of global economic growth, and further emphasised our resolve to promote secure and resilient ICT and critical infrastructure, which can contribute to regional security and stability” (ASEAN, 2018b).

Importance of the rules-based order

ASEAN member states recognise that their national security, stability and economic prosperity are closely linked to establishing an open, secure and peaceful ICT environment. It is not surprising then that ASEAN member states have a shared interest in participating in cyber norm discussions at the UN. The 2018 Statement of ASEAN and the Russian Federation on Cooperation in the Field of Security of and in the Use of Information and Communication Technologies stated that "the UN should play a leading role in promoting dialogue on the security of ICTs in their use by States and stress the importance of adopting rules, norms and principles of responsible behaviour of States in the use of ICTs" (ASEAN, 2018a).

Under the ASEAN Chairmanship of Singapore, member states reaffirmed the significance of the international rules-based order in cyberspace to maintain economic prosperity and better quality of life. Additionally, member states agreed in principle that practical confidence-building measures, voluntary and non-binding norms of State behaviour, and international standards are vital for stability in cyberspace at the 2018 AMCC. To this end, ASEAN members agreed to subscribe in principle to the 11 voluntary, non-binding norms of responsible state behaviour in cyberspace that were recommended by the 2015 UN GGE, and regional capacity building to implement these norms. ASEAN was the first and remains the only regional grouping to have adopted the UN's recommendations into their unique operations (Singapore Government Agency, 2018).

The concept of the rule law has been the cornerstone of ASEAN since its inception in 1967 and remains actively embraced by member states. It was first recognised in ASEAN's founding Bangkok Declaration document as a mechanism to maintain regional peace and stability; today, the concept of the rule of law is enshrined in the ASEAN Charter. Furthermore, the AMCC's decision to adopt the UN's recommendations aligns with ASEAN's ambition to implement the global cyber stability framework in the region and strengthen trust between member states (Singapore Government Agency, 2018).

It is essential to highlight the significance of this shared commitment, given ASEAN member states pursue individually differing ideological strategies to their domestic cybersecurity, as well as the fact only two ASEAN member states - Indonesia and Malaysia - had participated in earlier GGE's. Benjamin Ang (2018), a Senior Fellow at the Centre of Excellence for National Security has argued that,

> "The reiteration of the eleven UNGGE 2015 norms, instead of any other set of norms being proposed around the world, indicates that the region has made its clear choice upon which to develop policies and operations for cyberspace, in the midst of numerous other options, some of which are compatible with their values, and of some which are not".

By focusing cooperation in cyberspace on the UNGGE 2015 norms, ASEAN has established a clearly defined objective for the region to work towards. Efforts to overcome the challenges of different cyber capabilities, governance and policy among member-states can thus be addressed under this framework that aligns with Singapore's interests for a UN-led effort toward cyber cooperation.

Challenges to cyber strategy

The most pressing concern for ASEAN to address the evolving nature of cyber threats is the lack of a legal or regulatory framework on cybersecurity. Without a strict code of conduct or regulation, ASEAN's ambitions for a holistic and more coordinated approach to cybersecurity cooperation are restricted (Ramadhan, 2020). Arguably, the greatest challenge to establishing regional cyber governance for ASEAN lies within the diverging positions of its member-states. ASEAN constitutes an array of countries with diverse political regimes, contrasting degrees of economic development and differing levels of cyber maturity that frame their perception of cyberspace and its associated threats. As a result, the cyber domain has become a political arena where states reflect unique strategies and ambitions. With the challenges of regional heterogeneity in mind, we may consider the varying perspectives of ASEAN member-states on what constitutes cyberspace in relation to their national interests, such as the implementation of online content control and censorship policies in some member-states (Tran & Gomez, 2018).

Although the readiness of ASEAN as a regionally grouping to face the contemporary security issue remains questionable, this has not prevented the development of implementation road maps and master plans such as the ASEAN Cybersecurity Cooperation Strategy and ASEAN Master Plan (previous and current) (Timur, 2017). But - frameworks based on high-level guidelines for voluntary exchange and non-binding collaboration between government agencies are unlikely to be effective enough to secure the ASEAN cyber landscape; a tighter coordination mechanism is necessary (Kearney, 2018). For example, Singapore has advocated for the development of a regulatory and policy framework on cybersecurity for ASEAN that, in turn, would facilitate the integration of the ASEAN economy. This would require establishing cybersecurity standards and best practices to ensure regional interoperability (Choudhury, 2021). While ASEAN cannot demand compliance of its members, this does not mean the grouping is incapable of change. Instead, ASEAN relies on consensus to move forward, and the nature of this progress can be understood as slow and steady.

Capacity building measures (CBMs)

While norms require shared beliefs and principles, there is power in flourishing CBM's given they are based on a shared and practical interest in averting cyber conflict and/or conflict escalation amongst nations. Beyond building trust, ASEAN has strategically implemented specific CBM's aimed at supporting less developed members to enhance their respective cyber infrastructures and close the disparity gaps between member-states. The completed 2020 ASEAN CERT Maturity Framework study supported this initiative by identifying the systematic gaps where capacity-building efforts and training must be targeted (ASEAN, 2021). In doing so, these work to meet ASEAN's socio-economic objectives. It also encourages the establishment of shared perceptions in cyberspace and can provide an initial step toward developing regional norms to support a framework for cyber governance (Tran & Gomez, 2018).

ASEAN shares a collective focus on capacity building in cyberspace to address the structural challenges of technological, operational, political and legal disparities among member states. Capacity-building remains important in providing member states with the necessary capacity and ability to respond to current and newly emerging cyber threats. Implementing cyber CBM's is also necessary to minimise the threat of misconception and intensification in cyberspace. ASEAN Cybersecurity Ministers regularly meet and engage in ongoing informal forums to discuss practical ways to foster greater regional cybersecurity cooperation and facilitate capacity building (Koh, 2020). These forums include: (Koh, 2020).

- ASEAN Ministerial Conference on Cybersecurity (AMCC), held as part of the Singapore International Cyber Week (SICW)
- ASEAN Ministerial Meeting on Transnational Crime

- ASEAN Digital Ministers' Meeting
- ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies
- ASEAN Defence Ministers' Meeting Plus Experts' Working Group on Cyber Security
- ASEAN Working Group on Digital Data Governance

ASEAN states are enhancing regional cooperation on cyber capacity building through initiatives and programmes guided by the ASEAN Cybersecurity Cooperation strategy. These prominently function to build the region's capacity in protecting CII's, such as Industrial Control Systems, countering the use of ICTs for terrorist purposes, defending from cybercrime, among others. These initiatives and programs include: (Koh, 2020).

- ASEAN Cyber Capacity Development Project
- Digital Connectivity and Cybersecurity Partnership
- U.S-ASEAN Smart Cities Partnership
- ASEAN-Japan Cybersecurity Capacity Building Center
- ASEAN-Singapore Cybersecurity Center of Excellence
- US-ASEAN Connect Digital Economy Series
- ASEAN-China Partnership on Digital Economy Cooperation
- ASEAN-India Digital Work Plan

Beyond building the resilience of cyber infrastructure, capacity building programmes for information and expertise exchange are critical to forging a culture of transparency between ASEAN member-states. To this end, the 1st ASEAN Digital Ministers' Meeting held in 2021 approved Singapore-led initiatives on ASEAN Data Management Framework (DMF), ASEAN Model Contractual Clauses for Cross Border Data Flows (MCCs) and ASEAN CERT Information Exchange Mechanism. Singapore Minister Iswaran has said, "these tangible projects will help ASEAN businesses, especially the Small and Medium Enterprises (SMEs), seize the opportunities that the Digital Economy offers and strengthen our collective cybersecurity cooperation" (Ministry of Communications and Information, 2021). Moreover, unlike previous initiatives, the inclusion of MCC's allows for legally binding agreements between businesses when transferring intelligence and data across borders.

Singapore's role in ASEAN cybersecurity

To understand the imperative of ASEAN's cybersecurity agenda for Singapore, we need only examine the extensive ways the nation-state contributes to its facilitation. Singapore is indisputably a committed leader in strengthening ASEAN cybersecurity efforts and enhancing the ability of the region to respond to emerging international cyber threats. At the front line of ASEAN regional cybersecurity, Singapore embodies "the comprehensive outlook that the city-state is trying to advance in the region with respect to cyber issues, which blends areas of focus such as capacity-building, norm development, and joint research and intelligence sharing" (Parameswaran, 2018).

In collaboration with the Singapore International Cyber Week (SIWC) which facilitates multi-stakeholder dialogues on cybersecurity, Singapore hosts the annual ASEAN Ministerial Conference on Cybersecurity (AMCC) chaired by Singapore's Minister-in-charge of Cybersecurity. The AMCC is a platform that brings together the ASEAN Secretary-General and ASEAN Ministers of Telecommunications and/or Cybersecurity for non-formal discussions on cybersecurity concerns affecting the region and beyond (CSA, 2021a). Singapore also chairs the ASEAN Working Group on Digital Data Governance. Beyond the facilitation of regional dialogue, Singapore has also made significant monetary investments in regional capacity-building efforts, including the establishment of the ASEAN Cyber Capacity Programme (ACCP) in 2016. Singapore created a $10 million ASEAN Cyber Capacity Fund to improve regional cybersecurity capabilities, aligned with its desire for greater engagement in broader international discussions. By having within-region commitments from Singapore, ASEAN member states have had less need for external investment at the risk of increasing third-party influence (Putra, 2018; Heinl, 2019).

Singapore's commitment to regional cybersecurity was exemplified during its 2018 Chairmanship of ASEAN, which saw cybersecurity formulated as a key priority of its regional policy agenda. In recognition of the need for a formal ASEAN cybersecurity mechanism to enhance regional cyber coordination, the 2018 AMCC tasked Singapore with proposing a cybersecurity mechanism to guide inter-related cyber diplomacy, policy, and operational concerns (CSA, 2018a; CSA, 2019). Additionally, Singapore announced the establishment of the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) as an extension of the ASEAN Cyber Capacity Programme (ACCP). To strengthen the operational, policy, and legislative cyber-capacity efforts of ASEAN members, the S$30 million investment is based on three pillars: conduct research and provide training in areas spanning international law, cyber strategy, legislation, cyber norms, and other cybersecurity policy issues; provide CERT-related technical training as well as facilitate the exchange of open-source cyber threat and attack-related information and best practices; and conduct virtual cyber defence training and exercises (Singapore Government Agency, 2019). The ASCCE reflects a unifying stance by ASEAN member-states that cyber diplomacy efforts must align with operational issues such as information and data sharing. By addressing the coordination of regional cyber capacity-building efforts and implementing these measures, ASEAN states will give greater support to strengthen regional cooperation and position them to exert global influence with greater strategic clout as a regional grouping (Heinl, 2019). Furthermore to Singapore's Chairmanship of ASEAN, through close work with the UN Office of Disarmament Affairs (UNODA), Singapore announced the formation of a Singapore-UN Cyber Programme to develop and host annual workshops for building awareness of cyber norms and cyber policy scenario planning in ASEAN member states (Ministry of Foreign Affairs Singapore, 2018).

By taking on a leadership position on cybersecurity within ASEAN, Singapore has forged a favourable perception for itself among its partnering member states and the broader international community in enhancing cyber resilience. The nation-state has facilitated crucial cyber cooperative efforts between the UN and ASEAN member-states. Beyond the aforementioned Singapore-UN Cyber Programme, Singapore will be chairing the UN OEWG 2021-2025 and has already taken the opportunity to seek contributions from its ASEAN partners in this process. Speaking at the 2021 AMCC, Josephine Teo (2021) stated,

> I encourage AMS to actively contribute to the cyber stability framework – and collectively identify key issues of regional interest to value-add to the UN conversation. As Chair of the OEWG, Singapore looks forward to your support. We are keen to hear your candid views, and work with you to move the discussion toward our shared objective of a secure, resilient, and interoperable cyberspace.

Conclusion

The ASEAN grouping is a mechanism for security that has afforded shelter in an array of traditional and non-conventional issues since its inception. Singapore, as a small state, has benefited from the peaceful and conducive regional environment shaped by ASEAN. Against this backdrop, ASEAN provides Singapore with a platform to broaden its diplomatic clout by engaging larger, more powerful nations and entangling them within the ASEAN way that practises cooperation and dialogue. Singapore's Smart Nation initiative and economic prosperity are interdependent on securitising the ASEAN cyber landscape. For this reason, Singapore's strategic vision for a unified, forward and outward-looking approach to ASEAN cybersecurity has remained at the forefront of its regional ambitions.

Additionally, building the region's cyber resilience may also be a matter of preserving its reputation for Singapore. Singapore is geographically the smallest nation in the grouping, with limited natural resources and land space to its ASEAN counterparts. The city-state has leveraged this seeming disadvantage into strength and earned itself reputational standing as a regional hub for innovation and technological development "with its openness to trade, innovation-centric economy and skilled talent" (Hawksford, 2020). However, instability in the regional cyber landscape can potentially undermine this perception. Given the increasing strategic relevance of ASEAN, its positioning as key hubs for services, and widespread disparities in cyber capabilities, governance and policy, the region has become a vector for cyber-attack. As warned by Marsh's research, "cybercrime is becoming a greater risk in doing businesses in the Asia-Pacific as compared to the West. Cyber concern around the likelihood and impact of technological threats has sharpened among business executives in the Asia-Pacific (MarshMclennan, 2022).

It is acknowledged that member-states are dependent on each other to collectively deal with cyber issues to reap the full benefits of digital transformation. Moreover, if cyber issues continue to become more acute in the region without a proactive response, the impact on Singapore's global reputation and trade interests may be severe. Singapore is an indisputable regional leader in ASEAN in the sphere of cybersecurity through its facilitation of meetings on cybersecurity at a ministerial level, financial investments in capacity-building mechanisms and leadership position in forging closer cyber cooperative relations between ASEAN and the UN. These efforts will continue to support cybersecurity development in the ASEAN landscape to acquire securitisation. Additionally, maintaining its leadership position in regional cooperation on cyber issues will also support Singapore's influence in the international security environment. To bring this thesis to an end, the following chapter provides a comprehensive conclusion outlining the investigation's key findings.

Conclusion

This thesis has investigated how two important small Asia Pacific nations, New Zealand and Singapore, are seeking shelter from cyber insecurity and analyse the success made by the countries. Furthermore, it has sought to identify the similarities and differences in responding to cyber insecurity. So, how are New Zealand and Singapore, as small states, sheltering from cyber insecurity and are they being successful?

Firstly, it is evident that New Zealand is struggling to overcome significant resource challenges and technical obstacles, which are common vulnerabilities and limitations of small states. Unlike its larger counterparts, New Zealand faces hurdles to building a strong and capable cybersecurity workforce; cannot financially commit the necessary resources to successfully strengthen its cybersecurity and to advance technical expertise and knowledge in the sector to keep up with the evolving cyber landscape. On the other hand, Singapore has strategically prioritised cyber policy by upskilling its administrative competence and diplomatic expertise in the cyber sector. To this end, the small-city state has made significant investments in building a robust cybersecurity ecosystem and enacting regulatory policies to restrict the impacts of malicious cyber activity. Nonetheless, despite these extensive efforts to securitise Singapore's cyber landscape, the small state still faces challenges in adequately developing the required human resources to mitigate and respond to cyber threats. Additionally, the increasing disparity of cyber capabilities between small and larger powers means that small states are at greater vulnerability. While New Zealand and Singapore share a similar lack of capabilities in the cyber domain, their differing governmental systems demonstrate that liberal and illiberal democracies do not share all of the same challenges to acquiring cybersecurity. As an illiberal democracy, the Singaporean government has a greater capacity to adopt regulatory functions that restrict unfavourable behaviour and activity in the domestic cyber domain, such as the 2018 Cybersecurity Act. In contrast, New Zealand's democratic values of freedom present challenges to achieving a sustainable balance between privacy and security in cyberspace. These differences inform the degree of external shelter New Zealand and Singapore require.

Secondly, cyber issues are global in scope. Given the complex, transboundary nature of the cyber phenomenon, the pursuit of domestically focused foreign policy in cybersecurity cannot on its own address the external nature of the issue. The evidence in this thesis suggests that New Zealand and Singapore recognise this reality by adopting elements of sheltering in their cyber foreign policy approaches through memberships in regional arrangements and international organisations. Although the UN GGE and OEWG have made limited progress on cybersecurity beyond the 2015 implementation of informal norms and rules, there is potential for these efforts to develop and forge conventional international law in cyberspace. Evidently, these forums have allowed New Zealand and Singapore's cyber interests to be represented and contributed to the albeit informal development of internationally recognised understandings of cyberspace. As the international community continues these important multilateral discussions under the UN umbrella, there is an opportunity for small states to shape the development of global cooperation and the establishment of a regulatory framework or international treaty on state behaviour in cyberspace. New Zealand has the potential to leverage its independent status, international reputation in peace and disarmament and historical contributions to advancing nuclear non-proliferation treaties, to build on recent efforts at the UN and exercise international advocacy on these cyber issues. Maintaining Singapore's influential momentum in regional cyber cooperation and the broader international community will support Singapore's positioning to lead in future law-making processes of a universal legal mechanism for cybersecurity.

Third, developing collective security on cyber issues at the international level appears to be a slow process that faces challenges due to diverse ideological perspectives among the great powers and a lack of implementation of norms agreed to at the UN. As cybersecurity continues to grow in strategic importance in the wider pattern of cooperation, arguably, countries with more closely aligned strategic interests have made greater progress so far on issues around cybersecurity. Regional arrangements have provided a more substantive platform for small states to seek shelter in this context. The evidence in this investigation demonstrates that New Zealand's membership in the FVEY network remains integral to the country's ability to meet its national interests in security and intelligence. Larger counterparts in the arrangement provide tools and resources for the defence of the cyber domain, access to a greater pool of foreign intelligence, and security of the shared values of the liberal international rules-based order that would otherwise be unattainable for New Zealand. In the contemporary security environment, the ability of New Zealand to balance its relationship with the FVEYs and China has come into question. When New Zealand was partially frozen out of the FVEY arrangement by the US-based on conflicting policies in the 1980s, New Zealand could still rely on support from its other partners. As Chinese foreign interference becomes a greater concern to the stability of the liberal rules-based order, New Zealand needs to maintain its independent foreign policy credentials not to upset the views of its FVEY counterparts. A small state like New Zealand needs to be mindful of its partners' views, particularly as it navigates the complexities of great power competition between its traditional security partners – US, UK and Australia – while maintaining prosperity in its most important economic relationship with China.

Fourth, Singapore has established itself as an influential regional leader in cybersecurity within ASEAN. Continuous progress in facilitating cyber cooperation in the wider ASEAN region is imperative to the economic prosperity and national aspirations of Singapore. The regional organisation has afforded cooperation between member-states on cyber issues to develop capabilities, share technologies and forge collective mechanisms for the implementation of rules and norms. Singapore has successfully driven small state cooperation with its regional partners and has coupled these efforts with the wider international community. While global cooperation on cyber security issues is contingent upon compliance by larger powers, there is a positive role for small states to work collectively to forge a positive regional understanding that can, ideally, contribute to the emergence of similar understandings in other regions and, ultimately, to an international understanding.

Finally, what are promising research opportunities for the New Zealand and Singaporean cyber security literature in the future? Given that New Zealand has increasingly diversified its strategic interests throughout the Asia-Pacific region alongside its traditional liberal partners, the academic research would benefit from assessing new avenues of influence for New Zealand with other small states, such as ASEAN, and how they can collaborate diplomatically at the UN to put forward positions on cyber security that both find mutually beneficial. Strengthening relations around the development of cyber norms between the UN and Singapore would also be a fruitful route for research, as the latter is maneuvering itself into a position of influential leadership in the cyber domain internationally and seemingly has the capacity and expertise to share best practices with New Zealand.

Bibliography

- 60 Minutes Australia. (2021, May 30). *Dollar VS Democracy: Is China taking over New Zealand.* [video]. Retrieved from https://www.youtube.com/watch?v=8d3Lyk_vlW4.

- Ad'ha Aljunied, S. M. (2020). The securitization of cyberspace governance in Singapore. *Asian Security*, *16*(3), 343-362.

- Adams, A. (2016, May 5). *Budget 2016: $22.2m to boost cyber security.* Beehive. Retrieved from https://www.beehive.govt.nz/release/budget-2016-222m-boost-cyber-security.

- Alesina, A., & Spolaore, E. (2003). *The Size of Nations*. London and Cambridge: MIT Press.

- Anderlini, J. (2017, September 13). *China-born New Zealand MP probed by spy agency.* Financial Times. Retrieved from https://www.ft.com/content/64991ca6-9796-11e7-a652-cde3f882dd7b

- Ang, B. (2018). Next steps for cyber norms in ASEAN. S. Rajaratnam School of International Studies.

- Ann, S. (2020, October 7). *Opening Address by Ms Sim Ann, Senior Minister of State, Ministry of Communications and Information, at the Singapore International Cyber Week 2020 – Women in Cyber.* Retrieved from https://www.csa.gov.sg/news/speeches/sicw-2020-women-in-cyber.

- Archer, C., & Nugent, N. (2006). Introduction: Does the size of member states matter in the European Union?. *European Integration*, *28*(1), 3-6.

- Archer, C., Bailes, A & Wivel, A. (2014). *Small States and International Security: Europe and Beyond.* Routledge Taylor & Francis Group.

- Armstrong, H. W., & Read, R. (2000). Comparing the economic performance of dependent territories and sovereign microstates. *Economic Development and Cultural Change*, *48*(2), 285-306.

- ASEAN. (2018a). Statement of ASEAN and the Russian Federation on Cooperation in the Field of Security of and in the Use of Information and Communication Technologies. para. 6[Report]. Retrieved from https://asean.org/wp-content/uploads/2018/11/FINAL-Statement-of-ASEAN-and-the-Russian-Federation-on-Cooperation-in-the-Field-of-Security-of-and-in-the-Use-of-Information-and-Communication-Technologies.pdf

- ASEAN. (2018b, November 15). Chairman's Statement of the 13th East Asia Summit. https://asean.org/wp-content/uploads/2018/11/East_Asia_Summit_Chairman_Statement_Final.pdf.
- ASEAN. (2021). ASEAN Cybersecurity Cooperation Strategy 2021-2025. Retrieved from https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

- AsiaOne. (2011, September 21). *S'pore to set up National Cyber Security Centre*. Retrieved from https://www.asiaone.com/News/AsiaOne%2BNews/Singapore/Story/A1Story20110921-300765.html.

- Australian Government. (2010). *Australian Secredt Intelligence Service: Agency resources and planned performance.* Report. Retrieved from https://www.dfat.gov.au/sites/default/files/2010-11_ASIS.pdf

- Australian Government. (2015). *Australian Secret Intelligence Service: Entity resources and planned performance.* Report. Retrieved from https://www.dfat.gov.au/sites/default/files/2015-16-foreign-affairs-and-trade-pbs-asis.pdf

- Australian Government. (2021). *Australian Secret Intelligence Service: Entity resources and planned performance.* Report. Retrieved from https://www.dfat.gov.au/sites/default/files/pbs-2021-22-australian-secret-intelligence-service-asis.pdf

- Balakrishnan, V. (2018, September 29). *Speech by Minister for Foreign Affairs of the Republic of Singapore Dr Vivian Balakrishnan at the 73rd Session of the UN General Assembly New York.* [Speech]. Retrieved from https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/03/20220303-MFACOS2022-Min.

- Barak, O. (2009, May 29). Remarks by the President on Securing Our Nation's Cyber Infrastructure. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

- Barker, S. (2021, September 30). *The who's who of NZ's government & public cybersecurity agencies.* Security Brief New Zealand. Retrieved from https://securitybrief.co.nz/story/the-who-s-who-of-nz-s-government-public-cybersecurity-agencies

- Barkin, N. 2018, October 12. *Exclusive: Five Eyes intelligence alliance builds coalition to counter China.* Reuters. Retrieved from https://www.reuters.com/article/us-china-fiveeyes-idUSKCN1MM0GH

- Bloomberg. (n.d). *Can Small States Contribute to a Rules-based Order in Cyberspace?*. Retrieved from https://sponsored.bloomberg.com/article/cyber-security-agency/can-small-states-contribute-to-a-rules-based-order-in-cyberspace

- Bradley, A. (2021, June 15). *The rise of cybercrime and NZ's fragmented response*. RNZ. Retrieved from https://www.rnz.co.nz/news/in-depth/444735/the-rise-of-cybercrime-and-nz-s-fragmented-response.
- Brady, A. M. (2008). New Zealand-China relations: Common points and differences. *New Zealand Jounral of Asian Studies, 10*(2). 1-20
- Brady, A. M. (2017). *Magic Weapons: China's political influence activities under Xi Jinping* (Vol. 18). Washington, DC: Wilson Center.
- Brady, A. M. (2018). China in Xi's" New Era": New Zealand and the CCP'S" Magic Weapons". *Journal of Democracy*, *29*(2), 68-75.
- Brady, A. M. (2019). Small Can Be Huge: New Zealand Foreign Policy in an Era of Global Uncertainty. In *Small States and the Changing Global Order* (pp. 1-10). Springer, Cham.
- Brady, A. M. (2021). Magic Weapons and Foreign Interference in New Zealand: how it started, how it's going. *Policy Quarterly*, *17*(2).
- Brunatti, A. (2016). *The Architecture of Intelligence: Public Governance of the secret state in Australia, New Zealand and Canada.* [Doctoral thesis, Brunel University]. Brunel University Research Archive.
- Burton, J. (2017, June 3). *New Zealand's Agenda at the UN and other international organisations: international governance of cyberspace.* Retrieved from https://www.canterbury.ac.nz/media/documents/research/Burton_policybrief.pdf
- Burton, J. (2019). Small States and International Organisations: New Zealand's Diversifying International Engagement. In *Small States and the Changing Global Order* (pp. 307-324). Springer, Cham.
- Cabinet Minute. (March 28, 1985), *'Cabinet Submission 2635-ANZUS-Arragements for Handling Relations with the USA and New Zealand-Decision 5164' NAA:*

A14039/2635.

- CERT NZ. (2020). *2020 Report Summary.* [Quarterly Report]. https://www.cert.govt.nz/about/quarterly-report/2020-report-summary/.

- 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.

- Choudhury,. R. A. (2021, November 15). *What the world can learn from ASEAN's cyber cooperation.* GovInsider. Retrieved from https://govinsider.asia/resilience/what-the-world-can-learn-from-aseans-cyber-cooperation-amit-roy-choudhury/.

- Chua, G. S. & Dobberstein, N. (2020). *The ASEAN digital revolution.* A.T. Kearney. Retrieved from https://www.kearney.com/documents/20152/5364057/The+ASEAN+digital+revolution.pdf/625da4b5-8d05-6798-004a-e49a59e8d817?t=1581504740000

- CIO. (2021, July 6). *Enabling ASEAN's digital masterplan.* Retrieved from https://www.cio.com/article/188903/enabling-asean-s-digital-masterplan.html.

- Clark, D. (2021, December 13). *New border exception to support rapidly growing tech sector.* Beehive. Retrieved from https://www.beehive.govt.nz/release/new-border-exception-support-rapidly-growing-tech-sector.

- Collins, R., O'Connor-Close, C., & Zhang, A. (2020). Cyber incident cost estimates and the importance of building resilience. *Reserve Bank of New Zealand Bulletin*, *84*, 1-17.

- Coughlin, C. (2021, April 21). *Jacinda Ardern now Wests Woke Link.* The Daily Telegraph. Retrieved from https://www.telegraph.co.uk/news/2021/04/21/jacinda-ardern-now-wests-woke-weak-link/.

- Council on Foreign Relations. (2021, March 18). *Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?*. Retrieved from https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.

- Cox, J. S. (2013). *Canada and the five eyes intelligence community*. Canadian Defence & Foreign Affairs Institute.

- CSA. (2016, October 10). *Singapore's Cybersecurity Strategy 2016.* Retrieved from https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy.

- CSA. (2018a, September 18). *ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity-Building Efforts*. [Press Release]. Retrieved from https://www.csa.gov.sg/news/press-releases/amcc-2018.

- CSA. (2018b). Cybersecurity Act. Retrieved from https://www.csa.gov.sg/legislation/cybersecurity-act.

- CSA. (2019, October 2). *Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2019.* [Speech]. Retrieved from https://www.csa.gov.sg/News/Speeches/Asean-Ministerial-Conference-on-Cybersecurity-2019.

- CSA. (2021a, October 5). *The Singapore Cybersecurity Strategy 2021.* [Publications]. Retrieved from https://www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021.

- CSA. (2021b). *Singapore Cyber Landscape 2020.* [Report].

- CSA. (n.d,a). Our Organisation. Retrieved from https://www.csa.gov.sg/Who-We-Are/Our-Organisation.

- CSA. (n.d,b). *Youth Cyber Exploration Programme (YCEP).* Retrieved from https://www.csa.gov.sg/Programmes/SGCyberTalent/SGCyberYouth/YCEP.

- Cullen, M., & Reddy, P. (2016). Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand.

- Cyber Law Toolkit. (2021). *National position of Singapore.* Retrieved from https://cyberlaw.ccdcoe.org/wiki/National_position_of_Singapore_(2021).

- Deibert, R. J., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue*, *43*(1), 3-24.

- Domingo, F. C. (2016). Conquering a new domain: Explaining great power competition in cyberspace. *Comparative Strategy*, *35*(2), 154-168.

- DPMC. (2021, July 5). *New Zealand's Cyber Security Emergency Response Plan, Version 5, July 2021.* Retrieved from https://dpmc.govt.nz/sites/default/files/2021-08/New%20Zealands%20Cyber%20Security%20Emergency%20Response%20Plan.pdf.

- Eaton, J., & Kortum, S. (2002). Technology, geography, and trade. *Econometrica*, *70*(5), 1741-1779.

- Efrony, G. D. M, D. (2021, July 16). *The UN Cyber Groups, GGE and OWEG – A Consensus is Optimal, But Time of the Essence.* Just Security. Retrieved from https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/.

- Executive Office of the President: Office of Management and Budget. (2021, April 9). *FY2022 Discretionary Budget Request.* Retrieved from https://www.whitehouse.gov/wp-content/uploads/2021/04/FY2022-Discretionary-Request.pdf.

- Faafoi, K. (2018, November 22). *New qualification helps Kiwis get into cyber security careers. The New Zealand Government.* Retrieved from https://www.beehive.govt.nz/release/new-qualification-helps-kiwis-get-cyber-security-careers.

- Financial Markets Authority. (2021). *Market Operator Obligations Targeted Review – NZX: Findings from the FMA's targeted review of whether NZX is meeting its licensed market operator obligations.* [Report].

- Forsyth Jr, J. W., & Pope, B. E. (2014). Structural causes and cyber effects: Why international order is inevitable in cyberspace. *Strategic Studies Quarterly*, *8*(4), 112-128.

- Garvrilović, A. (2021, June 6). *What's new with cybersecurity negotiations? The UN GGE 2021 Report.* Diplo. Retrieved from https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-un-gge-2021-report/.

- GCSB. (2013, January 15). NZ-UK joint statement on cyber security. Retrieved from https://www.gcsb.govt.nz/news/nz-uk-joint-statement-on-cyber-security/.

- GCSB. (2017a). CORTEX FAQS. Retrieved from https://www.gcsb.govt.nz/our-work/information-assurance/cortex-faqs/.

- GCSB. (2017b). Malware Free Networks. Retrieved from https://www.gcsb.govt.nz/our-work/information-assurance/malware-free-networks-pilot/#:~:text=The%20GCSB's%20National%20Cyber%20Security,New%20Zealand' s%20cyber%20defence%20capabilities.

- GCSB. (2021). GCSB Women in STEM Scholarship. Retrieved from https://www.gcsb.govt.nz/working-for-us/gcsb-women-in-stem-scholarship/.

- GCSB. (2022). *History of the GCSB*. Retrieved from https://www.gcsb.govt.nz/about-us/history-of-the-gcsb/

- Gee, A., and Patman, R. 2021. "Small state or minor power? New Zealand's Five Eyes membership, intelligence reforms, and Wellington's response to China's growing Pacific role". *Intelligence and National Security, 36*(1), 34-50.

- Ghosh, N. (2019, April 23). *Singapore's cyber security chief says international norms, partnerships are key issues.* The Strait Times. Retrieved from https://www.straitstimes.com/singapore/singapores-cyber-security-chief-says-international-norms-partnerships-are-key-issues.

- Gold, J. (2021, March 18). *Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?. From Net Politics and Digital and Cyberspace Policy Program.* Retrieved from https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.

- Grigsby, A. (2017). The end of cyber norms. *Survival*, *59*(6), 109-122.

- Hampton, A. 2018. *A New Zealand perspective on cyber threats*. GCSB. Retrieved from https://www.gcsb.govt.nz/news/a-new-zealand-perspective-on-cyber-threats/.

- Hampton, A. (2019, April 5). *Improving the cyber security resilience of New Zealand businesses. Government Communications Security Bureau.* Retrieved from https://www.gcsb.govt.nz/news/improving-the-cyber-security-resilience-of-new-zealand-businesses/.

- Hampton, A. (2020, August 7). Speech: Cyber Security in a Covid-19 world. GCSB. [Speech]. Retrieved from https://www.gcsb.govt.nz/news/cyber-security-in-a-covid-19-world/.

- Hampton, A. (2021, February 1). *Successful GCSB STEM scholarships reflect diversity. Government Communications Security Bureau.* Retrieved from https://www.gcsb.govt.nz/news/successful-gcsb-stem-scholarships-reflect-diversity/.

- Hean, C. T. (2018, September 18). *DPM Teo Chee Hean at the Opening of the 3rd Singapore International Cyber Week.* [Speech]. Retrieved from https://www.mfa.gov.sg/Overseas-Mission/ASEAN/Press-Statements-Speeches/2018/09/Press_2018-09-18.

- Heinl, C. (2019, January 15). *An ASEAN way of cybersecurity: Unpacking the proposed ASEAN-Singapore Cybersecurity Centre of Excellence. Asia & the Pacific Policy Society.* Retrieved from https://www.policyforum.net/an-asean-way-of-cybersecurity/.

- Heng, Y. K. (2016). *Managing global risks in the urban age: Singapore and the making of a global city*. Routledge.

- Hensley, G. (2013). *Final approaches: a memoir*. Auckland University Press.

- Hill, J. F. (2012). A Balkanized Internet?: The Uncertain Future of Global Internet Standards. *Georgetown Journal of International Affairs*, 49-58.

- Hulsman, J. (2020, October 11). *The Anglosphere: The great power alliance right under Washington's nose.* Retrieved from https://thehill.com/opinion/national-security/519973-the-anglosphere-the-great-power-alliance-right-under-washingtons.

- IBM Security. (2022, February). *X-Force Threat Intelligence Index 2022.* [Report]. Retrieved from https://www.ibm.com/downloads/cas/ADLMYLAZ.

- Infocomm Development Authority. (2013). *National Cyber Security Masterplan 2018.* [Report]. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Singapore_2013_AnnexA.pdf.

- Insurance Journal. (2021, February 2). *How a 2020 Cyber Attack Brought the New Zealand Stock Exchange to Its Knees.* Retrieved from https://www.insurancejournal.com/news/international/2021/02/05/600216.htm.

- International Telecommunications Union. (2017). *Global Cybersecurity Index (GCI)*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

- ISC². (2020). *Cybersecurity Workforce Study, 2020.* [Report].

- Iswaran, S. (2018, August 6). *Statement by Mr S Iswaran, Minister-in-Charge of Cybersecurity, on the cyber-attack on SingHealth's IT system, during Parliamentary Sitting on 6 August 2018*. Singapore Government Agency. [Statement].

- Iswaran, S. (2020a, October 9). *Remarks by Mr S Iswaran, Minister for Communications and Information and Minister-in-charge of Cybersecurity at SICW 2020 Joint Press Conference.* [Press Conference]. Retrieved from https://www.csa.gov.sg/News/Speeches/sicw-2020-press-conference.

- Iswaran, S. (2020b, October 7). Opening Speech by S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the 5th ASEAN Ministerial Conference on Cybersecurity (live virtual broadcast) on 7 October 2020. [Speech]. Retrieved from https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/10/opening-speech-by-mr-s-iswaran-at-the-5th-asean-ministerial-conference-on-cybersecurity.

- Iswaran, S. (2020c, October 15). MCI's response to PQ on training cybersecurity experts for Singapore. Parliament QAs. Retrieved from https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/10/mci-response-to-pq-on-training-cybersecurity-experts-for-singapore?page=15

- Iyer, S & Mishra, S. (2021, June 2). *Understanding risks within Asia Pacific's growing cyber insurance market.* Verisk. Retrieved from https://www.verisk.com/insurance/visualize/understanding-risks-within-asia-pacifics-growing-cyber-insurance-market/

- Katzenstein, P. J. (2019). Corporatism and change. In *Corporatism and Change*. Cornell University Press.

- Keall, C. (2018, November 29). *'Not a ban' – Andrew Little offers hope for Huawei, but Spark dubious.* New Zealand Herald. Retrieved from https://www.nzherald.co.nz/business/not-a-ban-andrew-little-offers-hope-for-huawei-but-spark-dubious/YTS2AAOQ5YWKQWWIHK3G4IXAOU/

- Kearney, A. T. (2018). Cybersecurity in ASEAN: An urgent call to action. *Seoul: AT Kearney Inc*.

- Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, *38*(2), 7-40.

- Keohane, R. O. (1969). Lilliputians' Dilemmas: Small States in Internatinal Politics. *International organization*, *23*(2), 291-310.

- Keohane, R. O. (2005). 3. HEGEMONY IN THE WORLD POLITICAL ECONOMY. In *After Hegemony* (pp. 31-46). Princeton University Press.

- Keohane, R. O., & Martin, L. L. (1995). The promise of institutionalist theory. *International security*, *20*(1), 39-51.

- Key, J. (2013, August 21). *GCSB: Prime Minister John Key's speech.* Stuff. Retrieved from http://www.stuff.co.nz/national/politics/9070452/GCSB-Prime-Minister-John-

Keys-speech.

- Kim, S. (2014). Cyber security and middle power diplomacy: A network perspective. *The Korean Journal of International Studies*, *12*(2), 323-352.

- Kitteridge, R. (2019, April 11). *Director-General remarks: Justice Select Committee Inquiry into 2017 General Election and 2016 Local Elections.* Retrieved from https://www.nzsis.govt.nz/news/opening-remarks-justice-select-committee-inquiry-into-2017-general-election-and-2016-local-elections/.

- Koh, D. (2020, May 22). *Remarks by Mr David Koh, Chief Executive, Cyber Security Agency of Singapore, at the United Nations Security Council Arria Formula Meeting 2020, Cyber Security Agency of Singapore.* [Speech]. Retrieved from https://www.csa.gov.sg/news/speeches/unsc-arria-formula-meeting-2020.

- Koh, D. (2021). *Find a Friend, Bring a Friend: Singapore's Efforts on Cybersecurity. Centre For Strategic and International Studies*. [Podcast]. Retrieved from https://www.csis.org/podcasts/inside-cyber-diplomacy/find-friend-bring-friend-singapores-efforts-cybersecurity.

- Koh, T. (2018, January 9). *Why Asean is good for Singapore. The Strait Times.* Retrieved from https://cil.nus.edu.sg/wp-content/uploads/2018/01/Why-Asean-is-good-for-Singapore_The-Straits-Times.pdf

- Lan, T. (2020). Global cyber threats and the way ahead. In *New Zealand National Security: Challenges, Trends and Issues* (pp. 18-26). Massey University Press.

- Lim, H. (2017). *ASEAN and Member States: Transformation.* Retrieved from https://www.eria.org/3.11.ASEAN_50_Vol_3_Country_Reports_Singapore.pdf.

- Lindsay, J. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies, 22*(3), 383–384.

- Little, A. (2021, July 19). *New Zealand condemns malicious cyber activity by Chinese state-sponsored actors.* New Zealand Government. [Press Release] Retrieved from https://www.beehive.govt.nz/release/new-zealand-condemns-malicious-cyber-activity-chinese-state-sponsored-actors.

- Maass, M. (2017). Small states in world politics: The story of small state survival, 1648–2016. In *Small states in world politics*. Manchester University Press.

- Manantan, M. B. F. (2021). Advancing cyber diplomacy in the Asia Pacific: Japan and Australia. *Australian Journal of International Affairs*, *75*(4), 432-459.

- Maness, R. C., & Valeriano, B. (2016). The impact of cyber conflict on international interactions. *Armed Forces & Society*, *42*(2), 301-323.

- Markoff, M. (2021, May 31). Retrieved from https://twitter.com/MarkoffMichele/status/1398989931138228226

- MarshMcLennan. (2022). *Cyber Risk in Asia-Pacific – the Case for Greater Transparency.* Retrieved from https://www.marsh.com/kr/en/services/cyber-risk/insights/cyber-risk-in-asia-pacific-the-case-for-greater-transparency.html

- McGuire, M. (2021a). *New study highlights 100% rise in nation state cyberattacks in last three years.* HP Development. Press Release. Retrieved from https://press.hp.com/us/en/press-releases/2021/new-study-highlights-100-percent-rise-in-nation-state-cyberattacks.html>

- McGuire, M. (2021b). *Nation States, Cyberconflict and The Web of Profit.* Retrieved from https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf.

- Microsoft. (2022, April 27). *Special Report: Ukraine, An overview of Russia's cyberattack activity in Ukraine.* [Report]. Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

- Ministry of Communications and Information. (2021, January 22). *1st ASEAN Digital Ministers' Meeting approves Singapore-led initiatives on ASEAN Data Management Framework, ASEAN Model Contractual Clauses for Cross Border Data Flows and ASEAN CERT Information Exchange Mechanism.* [Press Release]. https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2021/1/1st-asean-digital-ministers-meetingNigital Ministers'.

- Ministry of Foreign Affairs Singapore. (2018, October 26). *STATEMENT ON BEHALF OF THE MEMBERS OF SOUTHEAST ASIAN NATIONS DELIVERED BY BURHAN GAFOOR, PERMANENT REPRESENTATIVE OF THE REPUBLIC OF SINGAPORE TO THE UNITED NATIONS, AT THE THEMATIC DEBATE ON CLUSTER FIVE: OTHER DISARMAMENT MEASURES AND INTERNATIONAL SECURITY OF THE FIRST COMMITTEE, 26 OCTOBER 2018*. Retrieved from https://www.mfa.gov.sg/Overseas-Mission/New-York/Mission-Updates/First_committee/2018/10/Press_20181026.

- Ministry of Foreign Affairs Singapore. (2022). *Cybersecurity.* Retrieved from https://www.mfa.gov.sg/SINGAPORES-FOREIGN-POLICY/International-Issues/Cybersecurity.

- Morgan, S. (2019, June 10). *Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021.* Cybercrime Magazine. Retrieved from https://cybersecurityventures.com/cybersecurity-market-report/.

- National Research Foundation. (2021). *National Cybersecurity R&D Programme.* Retrieved from https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme.
  Nationally Significant Organisations 2017-2018. [Report]. Retrieved from https://www.ncsc.govt.nz/resources/cyber-security-resilience-of-nzs-nationally-significant-organisations-2017-2018/.

- NCSC. (2018). *Cyber Security Resilience of New Zealand's Nationally Significant Organisations 2017-2018*. [Report]. Retrieved from https://www.ncsc.govt.nz/resources/cyber-security-resilience-of-nzs-nationally-significant-organisations-2017-2018/.

- NCSC. (2019). *Cyber Threat Report 2018/19. GCSB.* [Report]. Retrieved from https://www.ncsc.govt.nz/newsroom/cyber-threat-report-for-201819-released/.

- NCSC. (2020). *Cyber Threat Report 2019/20.* [Report]. Retrieved from https://www.ncsc.govt.nz/newsroom/cyber-threat-report-2020/.

- NordVPN. (2020). *Cyber Risk Index.* Retrieved from https://s1.nordcdn.com/nord/misc/0.13.0/vpn/brand/NordVPN-cyber-risk-index-2020.pdf.

- Nye, J. S. (1990). Soft power. *Foreign policy*, (80), 153-171.

- Nye, J. S. (2011). Nuclear lessons for cyber security?. *Strategic Studies Quarterly*, *5*(4), 18-38.

- NZ Government. (2017). Briefing to the Incoming Minister: Minister Responsible for the GCSB and Minister Responsible for the NZSIS.

- NZ Government. (2019). New Zealand's Cyber Security Strategy 2019. [Report]

- NZ Immigration. (2021). *Skill shortage list checker.* Retrieved from https://skillshortages.immigration.govt.nz/ict-security-specialist/.

- NZ Ministry of Business and Innovation. (2020, August 20). *Digital Technologies Industry Transformation Plan. Progress update for industry.* Retrieved from https://www.mbie.govt.nz/dmsdocument/11638-digital-technologies-industry-transformation-plan.

- NZ Ministry of Foreign Affairs and Trade. (2019). *Key facts on New Zealand-China trade.* Retrieved from https://www.mfat.govt.nz/kr/trade/free-trade-agreements/free-trade-agreements-in-force/nz-china-free-trade-agreement/key-facts-on-new-zealand-china-trade/.

- NZ Ministry of Foreign Affairs & Trade. (2020, December 1). The Application of International Law to State Activity in Cyberspace. [Report]. Retrieved from https://www.mfat.govt.nz/assets/Peace-Rights-and-Security/International-security/International-Cyber-statement.pdf.

- NZ Parliament. (2013, August). Government Communications Security Bureau and Related Legislation Amendment Bill. Retrieved from https://www.parliament.nz/en/pb/bills-and-laws/bills-proposed-laws/document/00DBHOH_BILL12122_1/government-communications-security-bureau-and-related-legislation.

- NZ Parliament. (2021, June 29). *Urgent Debate – Ransomware Attack – Waikato District Health Board.* [Transcript]. Retrieved from https://www.parliament.nz/en/pb/hansard-debates/rhr/combined/HansDeb_20210629_20210629_20.

- NZ Treasury. (2010). Vote Communications Security and Intelligence 2020/11.[Report]. Retrieved from https://www.treasury.govt.nz/sites/default/files/2011-05/suppest11comsec.pdf.

- NZ Treasury. (2015). Vote Communications Security and Intelligence 2015/16. [Report]. Retrieved from https://www.treasury.govt.nz/sites/default/files/2016-05/suppest16comsec.pdf.

- NZ Treasury. (2020, May 14). Vote Communications Security and Intelligence - Finance and Government Administration Sector - Estimates 2020/21. [Report]. Retrieved from https://www.treasury.govt.nz/publications/estimates/vote-communications-security-and-intelligence-finance-and-government-administration-sector-estimates-2020-21-html.

- 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.

- Office of the Director of National Intelligence. (2017, January 6). *Assessing Russian Activities and Intentions in Recent US Elections*. Intelligence Community Assessment. [Report]. Retrieved from https://www.intelligence.senate.gov/publications/assessing-russian-activities-and-intentions-recent-us-elections.

- Office of the Director of National Intelligence. (n.d). *U.S Intelligence Community Budget.* Retrieved from https://www.dni.gov/index.php/what-we-do/ic-budget.

- Omand, D. (2018). The threats from modern digital subversion and sedition. *Journal of Cyber Policy*, *3*(1), 5-23.

- Panke, D. (2012). Small states in multilateral negotiations. What have we learned?. *Cambridge Review of International Affairs*, *25*(3), 387-398.

- Paterson, T., & Hanley, L. (2020). Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'. *Australian Journal of International Affairs*, *74*(4), 439-454.

- Peters, W. (2018, November 16). *Australia and New Zealand announce joint Pacific Cyber cooperation.* Beehive. [Press Release]. Retrieved from https://www.beehive.govt.nz/release/australia-and-new-zealand-announce-joint-pacific-cyber-cooperation.

- Peters, W. (2018, November 16). *Australia and New Zealand announce joint Pacific Cyber cooperation.* Beehive. Retrieved from https://www.beehive.govt.nz/release/australia-and-new-zealand-announce-joint-pacific-cyber-cooperation.

- Ponti, J. (2021, April 14). *David Koh, Chief Executive, Cyber Security Agency on building cybersecurity capacities in Singapore and the ASEAN.* OpenGov. Retrieved from https://opengovasia.com/david-koh-chief-executive-of-the-cyber-security-agency-on-building-cybersecurity-capacities-in-singapore-and-the-asean/.

- Putt, S. (2021, May 7). *NZ Fry Up: Cybersecurity skills shortage; Data on NIWA's mind; Growing NZ IT talent.* Computer World. Retrieved from https://www.computerworld.com/article/3618172/nz-fry-up-cybersecurity-skills-shortage-data-on-niwas-mind-growing-nz-it-talent.html.

- Ramadhan, I. (2020). Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN). *Journal of Social and Political Sciences*, *3*(4).

- Robinson, J. (2021, July 9). *Cyberwarfare statistics: A decade of geopolitical attacks.* Privacy Affairs. Retrieved from https://www.privacyaffairs.com/geopolitical-attacks/.

- Rõigas, H. & Minárik, T. (2015). *2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law.* The NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.

- Rokkan, S., & Urwin, D. W. (1983). *Economy, territory, identity: Politics of West European peripheries*. London; USA; New Delhi: Sage Publications (CA).

- Rothstein, R. (1968). *Alliances and small Powers.* New York: Columbia University Press.

- Schmitt, M. (2021, June 10). *The Sixth United Nations GGE and International Law in Cyberspace.* Just Security. Retrieved from https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

- Segal, A., Akimenko, V., Giles, K., Pinkston, D. A., Lewis, J. A., Bartlett, B., ... & Noor, E. (2020). The Future of Cybersecurity across the Asia-Pacific. *asia policy*, *15*(2), 57-114.
- Sin, B. (2017, March 21). *What Huawei's NZ$400M Investment in New Zealand Means For The Country's Networks.* Forbes. Retrieved from https://www.forbes.com/sites/bensin/2017/03/21/what-huaweis-nz400-million-investment-in-new-zealand-means-for-the-countrys-networks/?sh=1ac93b825e4e.
- Singapore Government Agency. (2019, October 2). *Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2019.* [Speech]. Retrieved from https://www.csa.gov.sg/News/Speeches/Asean-Ministerial-Conference-on-Cybersecurity-2019.
- Singapore News Center. (2018, May 18). *Cybersecurity threats to cost organisations in Singapore US$17.7 billion in economic losses.* Microsoft. Retrieved from https://news.microsoft.com/en-sg/2018/05/18/cybersecurity-threats-to-cost-organisations-in-singapore-us17-7-billion-in-economic-losses/.
- Smart Nation Singapore. (2018). *Smart Nation Strategy*. Retrieved from https://www.smartnation.gov.sg/files/publications/smart-nation-strategy-nov2018.pdf.
- Stapleton-Gray, R., & Woodcock, W. (2011). National internet defense---small states on the skirmish line. *Communications of the ACM*, *54*(3), 50-55.
- Statista. (2021). *Leading countries in the Globalization Index field of economic globalization 2021.* Retrieved from https://www.statista.com/statistics/268171/index-of-economic-globalization/.
- Steff, R. & Dodd-Parr, F. (2019) Examining the immanent dilemma of small states in the Asia-Pacific: the strategic triangle between New Zealand, the US and China, *The*

*Pacific Review, (32)*1, 90-112, DOI: 10.1080/09512748.2017.1417324.

- Stevens, T. (2012). A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy*, *33*(1), 148-170.

- Súilleabháin, A. Ó. (2013, June 11). *Small States Bring Big Ideas to the United Nations.* The Global Observatory. Retrieved from https://theglobalobservatory.org/2013/06/small-states-bring-big-ideas-to-the-un/.

- Súilleabháin, A. Ó. (2014). *Small states at the United Nations: diverse perspectives, shared opportunities*. New York: International Peace Institute.

- Teo, J. (2021, October 16). Keynote Address by Mrs Josephine Teo, Minister for Communications and Information, at ASEAN Ministerial Conference on Cybersecurity on 6 October 2021. [Speech]. Retrieved from https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2021/10/keynote-address-by-mrs-josephine-teo-at-asean-ministerial-conference-on-cybersecurity.

- Tertiary Education Commission. (2020, December 18). Targeted Training and Apprenticeship Fund (free trades training). Retrieved from https://www.tec.govt.nz/funding/funding-and-performance/funding/fund-finder/targeted-training-and-apprenticeship-fund/.

- The Strait Times. (2018, November 29). *New Zealand says Huawei ban not because it's Chinese.* Retrieved from https://www.straitstimes.com/asia/australianz/new-zealand-says-huawei-ban-not-because-its-chinese.

- The Strait Times. (2020, November 4). *Singapore to work with UN to help nations implement norms for responsible cyber behaviour.* Retrieved from https://www.straitstimes.com/tech/singapore-to-work-with-un-to-help-nations-implement-norms-for-responsible-cyber-behaviour.

- The World Bank. (2020). *Individuals using the Internet (% of population)*. Retrieved from https://data.worldbank.org/indicator/IT.NET.USER.ZS?most_recent_value_desc=false.

- Thorhallsson, B. (2012). Small states in the UN Security Council: means of influence?. *The Hague Journal of Diplomacy*, *7*(2), 135-160.

- Thorhallsson, B., & Steinsson, S. (2018). The theory of shelter. *Small States and Shelter Theory: Iceland's External Affairs*, 24-58.

- Timur, F. G. C. (2017). The Rise of Cyber Diplomacy ASEAN's Perspective in Cyber Security. *KnE Social Sciences*, 244-250.

- Tong, C. Y. (2000, April 5). *Strategies to Develop Singapore into an Infocomm Hub*. Infocomm Media Development Authority. Retrieved from https://www.imda.gov.sg/news-and-events/Media-Room/archived/ida/Speeches/2000/20060926102508.

- Tran Dai, C., & Gomez, M. A. (2018). Challenges and opportunities for cyber norms in ASEAN. *Journal of Cyber Policy*, *3*(2), 217-235.

- Treasury Board of Canada Secretariat. (2010). 2010-11 Estimates: The Government Expense Plan and The Main Estimates. Report. Retrieved from https://www.tbs-sct.canada.ca/est-pre/20102011/me-bpd/toc-tdm-eng.pdf

- Treasury Board of Canada Secretariat. (2022, May 20). *Infographic for Canadian Security Intelligence Service.* Retrieved from https://www.tbs-sct.canada.ca/ems-sgd/edb-bdd/index-eng.html#infographic/dept/94/financial/.

- UN. (2015). Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons. Retrieved from https://www.un.org/en/conf/npt/2015/pdf/background%20info.pdf.

- UN. (2019). *Singapore's views on developments in the field of information and telecommunications in the context of international security, pursuant to general assembly resolutions 73/27 and 73/266.* Retrieved from https://www.un.org/disarmament/wp-content/uploads/2019/09/Singapore-2019.pdf.

- US National Security Agency. 2007. *"Cryptologic Almanac 50th Anniversary: Six Decades of Second Party Relations." Declassified and approved for release by the NSA, February 27.* Retrieved from https://www.nsa.gov/news-features/declassified-documents/crypto-almanac-50th/assets/files/six_decades_of_second_party_relations.pdf.

- Van der Meet, S. (2016, December). *Medium-sized states in international cyber security policies.* Clingendael: Netherlands Institute of International Relations. Retrieved from https://www.clingendael.org/sites/default/files/pdfs/PB_Medium_sized_states_international_cyber_security.pdf

- Vayrynen, R. (1971). On the definition and measurement of small power status. *Cooperation and Conflict*, *6*(1), 91-102.

- Vital, D. (1971). *The survival of small states: Studies in small power/great power conflict.* Oxford University Press

- Vucetic, S. (2010). Anglobal governance?. *Cambridge Review of International Affairs*, *23*(3), 455-474.

- Wagenseil, P. (2011, February 17). *Cyberwarfare Called Fifth Domain of Battle by Pentagon.* NBC News. Retrieved from https://www.nbcnews.com/id/wbna41627487.

- Walstad, L. (2021, August 10). *The Best Cities For A Cybersecurity Job.* TechShielder. Retrieved from https://techshielder.com/the-best-cities-for-a-cybersecurity-job.

- Wellings, B., & Mycock, A. (2019). *The Anglosphere: Continuity, Dissonance and Location*. Oxford University Press.

- Wivel, A. (2000). Theory and Prospects for Northern Europe's Small States. *Cooperation and Conflict*, *35*(3), 331-340.

- Yang, B, L. (2006, June 20). *iN2015: Singapore. An Intelligent Nation, A Global City, Powered By Infocomm.* Singapore Government Agency. Retrieved from https://www.imda.gov.sg/news-and-events/Media-Room/archived/ida/Speeches/2006/20050714101409.

- Yang, Y. (2019, March 5). *Is Huawei compelled by Chinese law to help with espionage*?. Financial Times. Retrieved from https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0