Improving Cyber Defence for Critical National Infrastructure in New Zealand

A thesis

submitted in partial fulfilment of the requirements for the degree

of

Master of Cyber Security - Computing & Mathematical Sciences

at

The University of Waikato

by

BHOJRAJ SINGH PARMAR

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

January 2024

This page intentionally left blank.

Abstract

The challenge of securing comprehensive services enabled by cyber-physical technologies is becoming increasingly acute. Industrial Control Systems (ICS) and Operational Technology (OT) environments have been in place for several decades. With a combination of computer software, hardware components and industrial/commercial use, these systems are essential in the control and automation of countless industrial procedures and processes that provide indispensable human services in most countries; they make it possible to operate and maintain such operations as the flow of energy through power grids, the treatment and supply of clean water to billions of people, and the maintenance of life saving medical facilities around the world.

This research aims to critically analyse New Zealand's existing cybersecurity strategies and approaches in its defence of Critical National Infrastructure (CNI) organisations operating OT and ICS environments. In this regard, the research draws on international best practices, and proposes a set of hypotheses and actionable insights to fortify cyber resilience for CNIs. It also explores how government-enforced frameworks and standards improve cyber defence for CNIs along with improved accountability. Learnings from this research may be used by policy makers, cyber security leaders, and the government of New Zealand in their consideration of and consultations on academic and pragmatic application, for the development or adoption and enforcement of cyber security standards for CNIs in New Zealand. The essence of this thesis lies in its commitment to contributing to the broader discourse on cybersecurity for OT and ICS environments--particularly in safeguarding critical infrastructures--thereby enhancing the security and welfare of nations in a dynamically changing threat landscape.

To achieve the aforementioned aim, this thesis undertakes an analysis of cyber security standards and frameworks that governments around the globe--especially within the countries represented in the Five Eyes intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States--have enforced for CNIs operating OT and ICS environments. Additionally, the thesis examines whether there are other geographies that are a closer fit culturally and economically for New Zealand to learn from and to emulate when it comes to considering future strategies for improving cyber defence for CNIs. This thesis further explores how systematic, strategic, and collaborative

efforts in combination with government enforced frameworks and standards improve cyber defence for CNI and OT and ICS environments. It is guided by comparative analysis, utilizing both qualitative and quantitative data, including policy document reviews, expert interviews, and studies of international best practices.

TABLE OF CONTENTS

1 Purpose and Acknowledgement

This thesis fulfils partial requirements for the completion of Master of Cyber Security degree at the University of Waikato. The research has been conducted and the thesis authored by Bhojraj Parmar, who has acquired a breadth of experience in digital and operational technology industries for over two decades, the majority of which has been spent in protecting critical infrastructure and sensitive information systems from cyber threats. The author would like to acknowledge the invaluable guidance and unwavering support that Dr. Vimal Kumar provided throughout the development of this thesis. His expertise and mentorship have been fundamental in steering this research towards meaningful and impactful conclusions. Additionally, the author would like to sincerely thank the ethics committee at the University of Waikato, which helped to define privacy measures in advance for the surveys conducted and finally, a sincere and heartfelt token of gratitude to all the industry experts in Aotearoa who contributed their precious time and candidly shared their opinions and thoughts on making this effort meaningful.

2 Introduction

Any modern society trying to innovate and navigate the ongoing waves of digital and technological advancements is at risk of becoming a victim of complacency in some areas as it advances in others. Innovation and change have become the only constants in recent times where new and creative use cases for cyber-physical exploitation of technology are constantly challenging the current state. In this landscape of dynamic changes, governments around the world are trying to keep up with new challenges as they endeavour to offer better, simpler, and more accessible services to their people and organisations while keeping up with the need to increase rigor in protecting information and safety in this digital first world.

Critical services such as access to energy, water, transportation, healthcare, food, telecommunications, and finance have evolved greatly in the last few decades. The evolution has been shaped primarily through technology -- specifically computers and cyber-physical devices referred to as Internet of Things (IoT) and Industrial IoT (IIoT). Systems, environments, and digital solutions enabling these critical human services such as clean water, electricity, transportation, health services and communication infrastructure are generally referred to as Critical National Infrastructure (CNI) throughout this thesis. Industrial Controls Systems (ICS) and Operational Technology (OT) are broadly referred to as devices, systems, controls, automation systems and mechanisms that operate the environments offering essential services to the functioning of modern society. ICS and OT environments empower the operation of many CNIs. Use of ICS and OT systems has enabled many modern infrastructures to evolve and become so reliable that human health and safety are themselves safeguarded by technology. Examples of such systems include water quality monitoring, electricity distribution, and health care monitoring systems for critical care and vulnerable patients. In recent years, the evolution of networks, internet, software and cyber-physical systems has pushed the operation of ICS and OT systems to be managed through digital systems.

Historically, water, electricity and gas distribution did not rely greatly, if at all, on software or digital platforms. However, innovation and business needs for interconnectedness are well justified in the current economic landscape. For example, in the energy sector it was realised that consumers benefit from real time access to their electricity usage and billing information as this helps them become more conscious of their role in contributing to a

more sustainable future. Additionally, New Zealand's commitment to sustainability has led to a rapid evolution of its energy sector, particularly through the adoption of smart grid technologies and increased use of sustainable energy sources. And global influence has led to an increase in EV charging applications and systems. Similar changes in such areas as consumer demand, New Zealand's commitment to sustainability, quality of life, and global trends have created the need for efficient operation and delivery of critical services. As a result, similar innovations are currently being implemented or considered for the water, transportation, and health sectors in New Zealand. All of these drivers for change require that the legacy or analogue systems that operated the country's CNI services evolve or are augmented with digital systems and software that provide better precision, quality and efficiency. And this comes at a cost of increased risk of cyber-attacks and intrusions that traditional and modern computer systems face.

CNIs are essential to the functioning of modern society, but they are also increasingly vulnerable to cyber-attacks. These systems are marvellous engineering achievements. However, the threat landscape in digital technology that supports their control and management has evolved considerably faster than the advancement of security controls for ICS and OT software and hardware. Therefore ICS/OT environments are particularly vulnerable, as they are often legacy systems that were not designed with security in mind. In many industries these systems required no connectivity, data movement, or operational integration into any corporate, data analysis, or productivity systems. However, with the increased need and business justification to consume data for real time monitoring, management, maintenance, pricing, or regulatory requirements, and the efficiencies noted above, many of the OT systems have some form of connectivity or routing of digital traffic in and out of the ICS/OT environments of most of the CNIs. In the industry, this is also referred to as IT and OT convergence. This convergence, although necessary in the current state of evolution of technology and services, possesses new cyber security risks. In the efforts to boost productivity and exploit more business use cases through data collection, the business decision-makers have not put adequate thought into securing the mechanism which enables this convergence.

From the researcher's own experience in the OT/ICS cyber security industry and in defence of the business decision makers, no considerable effort has been made to train and raise awareness to help them ask meaningful questions. For example, when trying to create convergence or integration points into a water purification facility and distribution systems

in an urban area, asking if enabling real time consumption of the pressure valve data and water quality system can allow a malicious actor the ability to poison the water is surely an important question. If the answer is not an absolute "NO" from digital or technology teams then the business personnel must be enabled, trained, and encouraged to ask, "What measures can be taken to ensure the safety of our people while we try to achieve this business outcome?" These are tough questions to ask and hard conversations to have. For organisations, compliance can be achieved through education and awareness programs. However, for a nation it becomes a lot more challenging to systematically defend critical infrastructure wherever adequate consideration or enforcements are not employed when modernising ICS/OT systems.

In recent years there has been a general increase in awareness about the threats that CNI face if cyber security is not considered a priority. For example, many nations acknowledged the vulnerabilities and the impact of cyber-attacks on citizens when Ukraine experienced a targeted cyber-attack in 2015 in which a large number of citizens were adversely affected as attackers disrupted the distribution of electricity. An analysis from the International Society of Automation (ISA), undertaken in an article titled *Lessons Learned From a Forensic Analysis of the Ukrainian Power Grid Cyberattack* authored by Patrice Bock, Jean-Pierre Hauet, Romain Françoise, and Robert Foley, published on the ISA Interchange blog[i], concluded that the attackers exploited some basic flaws in security control design and were able to remain undetected for a long period of time, which allowed them to learn the operating environment and exploit system and process weaknesses to carry out an impactful attack which affected a large population.

In December 2018, Kevin Hemsley, CISSP and Dr. Ronald E Fisher from the National and Homeland Security, Idaho National Laboratory (INL), published a study titled *History of Cyber Incidents and Threats to Industrial Control Systems*[ii] to shed light on the growing cyber threats to ICS devices that support OT environments in many of the CNIs around the world. Their analysis included open source, cyber security companies, news media, independent security researchers, governments, and other published reports. It provides an insightful summary of 23 instances of threats between the years 1903 and 2017, posed directly to industrial controls systems through the means of digital tactics, tools, and procedures (TTPs). The following table provides a list of the instances reported in this study:

Table 1: ICS Cyber Incidents in the INL Study: (Hemsley, 2018)

Year	Type	Name	Description	Industry / sector
2000	Attack	Maroochy Water	A disgruntled employee used radio frequency (RF) signals to disrupt the Maroochy Shire Council's wastewater system.	Water and wastewater
2008	Attack	Turkey Pipeline Explosion	The explosion of a segment of the Baku-Tbilisi-Ceyhan (BTC) Oil Pipeline was attributed to a cyber-attack, but this has been disputed.	Energy
2010	Malware	Stuxnet	A sophisticated malware that targeted Iranian nuclear centrifuges.	Energy
2010	Malware	Night Dragon	A series of cyber-attacks targeting global oil, energy, and petrochemical companies.	Energy
2011	Malware	Duqu/Flame/Gauss	A family of malware used to steal information from industrial control systems.	Energy, Manufacturing, Water and wastewater
2012	Campaign	Gas Pipeline Cyber Intrusion Campaign	A series of cyber-attacks targeting natural gas pipeline sector companies.	Energy
2012	Malware	Shamoon	Malware used to target large energy companies in the Middle East, including Saudi Aramco and RasGas.	Energy
2013	Attack	Target Stores	Hackers gained access to Target's point-of-sale systems through a third-party HVAC vendor.	Retail
2013	Attack	New York Dam	The U.S. Justice Department claims Iran conducted a cyber-attack on the Bowman Dam in Rye Brook, NY.	Other
2013	Malware	Havex	A malware campaign targeting industrial control systems.	Energy
2014	Attack	German Steel Mill	A cyber-attack resulted in massive damage to a German steel mill.	Manufacturing

Year	Type	Name	Description	Industry / sector
2014	Malware	Black Energy	A malware campaign targeting human-machine interfaces (HMIs) in industrial control systems.	Energy
2015	Campaign	Dragonfly/Energetic Bear No. 1	Ongoing cyber-espionage campaign, Bear No. 1 primarily targeting the energy sector.	Energy
2015	Attack	Ukraine Power Grid Attack No. 1	The first known successful cyber-attack on a country's power grid.	Energy
2016	Attack	"Kemuri" water company	Attackers gained access to hundreds of programmable logic circuits (PLCs) used to manipulate control applications and altered water treatment chemicals.	Water and wastewater
2016	Malware	Return of Shamoon	A second Shamoon malware attack targeted Saudi Arabia's civil aviation agency and other Gulf State organisations.	Aviation
2016	Attack	Ukraine Power Grid Attack No. 2	Cyber-attackers tripped breakers in 30 substations, turning off electricity to 225,000 customers.	Energy
2017	Malware	CRASHOVERRIDE	The malware used to cause the Ukraine power outage was finally identified.	Energy
2017	Group	APT33	A cyber-espionage group targeting the aviation and energy sectors.	Aviation, Energy
2017	Attack	NotPetya	A malware attack that targeted the Ukraine by posing as ransomware, but with no way to pay a ransom to decrypt altered files.	Energy
2017	Campaign	Dragonfly/Energetic Bear No. 2	A cyber-espionage campaign targeting the energy sector.	Energy
2017	Malware	TRITON/Trisis/HatMan	Industrial safety systems in the Middle East targeted by sophisticated malware.	Energy

According to Brodt, O. (2023, October 16). *A brief history of ICS-tailored attacks*[iii] such attacks have continued. To illustrate the point, the researcher has added additional key events, outlined in table 2, below, for a more recent outlook:

Table 2: ICS Cyber Incidents 2020 Onwards

Year	Type	Name	Description	Industry / sector
2020	Attack	Water Filtration Plant	A pump went into continuous operation at one site and data was changed at another to manipulate water quality data to increase the amount of chlorine in the drinking water. [iv]	Water
2021	Attack	Colonial Pipeline	A ransomware operator encrypted computer systems critical to business operation and pipelines were shutdown (not directly compromised) to prevent impact. [v]	Energy - Oil and Gas
2022	Malware	INDUSTROYER2	Purpose built for substation disruption capabilities[vi]	Energy
2022	Malware	INCONTROLLER	A rare and dangerous set of tools with capabilities to impact process, control, and physical safety of ICS and OT environments [vii]	Various

A leading threat intelligence service provider, Mandiant (now part of Google Cloud), published a report[viii] earlier this year highlighting how nation state threat actors have been investing in upskilling and increasing capabilities within their cyber operations to compromise and impact OT systems. The report highlights the evidence in relation to government-backed entities that are funding and securing services to develop frameworks and training material aimed at gaining control and/or causing disruption to OT environments.

Mandiant published another report on zero-day vulnerabilities in the wild (2012 to 2022)[ix], which clearly indicates that an increasing number of zero-day vulnerabilities are being discovered and exploited in the wild. Many of these vulnerabilities directly or indirectly impact the security of ICS/OT environments operating critical services within CNIs across the globe and in New Zealand.

Another leading ICS/OT cyber security service provider, Dragos, notes in its yearly report for ICS/OT vulnerabilities trends for 2022[x] that there has been a considerable increase in discovered vulnerabilities in ICS and OT environments over the years.

When further observing the TTPs used in most of the attacks and malware listed in Table 1 and Table 2 above, it is evident that there is no such thing as a "fully air gapped" network. "Fully air gapped" is a term used to denote that there is a part of the network or system that is not connected to or reachable from any other computer network. If this were true, most of the incidents noted above would have been unsuccessful. This is all the more concerning in OT and ICS environments because service interruption may not only have a bearing on data flow but also has a direct impact on people's lives and safety. If a gas leak detection sensor in a refinery is under the control of a threat attacker, this could lead to an explosion affecting the lives of everyone in that facility. If an attacker brings down an electric grid, it can impact the supply of electricity to many lifesaving facilities and a prolonged outage may pose danger to life and the outage of many other critical services. Consequently, cyber-attacks and/or loss of control do not have the same impact in OT environments that operate many CNI services as they would in most corporate digital systems.

3 Motivation

3.1 Evolving Threat Landscape

Recent cyber-attacks on the Waikato Health Board systems[xi], Auckland Transport ticketing system[xii] and New Zealand Exchange[xiii] are noteworthy as these directly impacted people and critical services such as health, transportation, and financial services. This increase in targeted attacks is in line with the global uptick, caused primarily by financially motivated threat actors who rely on extortion as a means to achieve their mission. Financially motivated threat actors use ransomware, data theft, and service disruption -- sometimes in combination -- to pressure organisations to pay a certain amount in cryptocurrency to return to operation or to prevent public disclosure of sensitive information.

3.2 The Unknown Size of the Problem

In New Zealand, there is no mandatory reporting of cyber security incidents and vulnerabilities enforced for any CNIs operating in the private sector, which comprises the majority of utilities and other critical services. Although the government of New Zealand gathers threat intelligence from domestic and international partners, the actual size of the problem is unknown when it comes to cyber-attacks and financial loss. CERT NZ publishes a quarterly report for reported incidents, but most of these reports are voluntary and the insights published do not specify how many of these attacks or how much of the financial loss was suffered within the CNIs. CERT NZ publishes a regular summary of reported cyber security incidents. In the Q2 2023 report[xiv] it notes a 1% decrease in incidents responded to by CERT NZ from Q1 2023 and reports an indirect financial loss of $4.2 million dollars. Although useful and of value for general awareness, these figures do not represent the size of the problem and the real threat landscape as many organisations may have suffered from cyber-attacks and even paid ransom to threat actors without reporting the incidents to CERT NZ or making them public through the media. With the lack of reporting requirements and visibility over the current state of loss and impact of threats faced by CNIs – especially where OT/ICS environments are targeted or impacted – the New Zealand government and the private sector alike are unable to put forth strong business cases to secure the general buy-in, funding, and heightened vigilance required to defend CNIs.

3.3 Lack of a Cohesive Approach

The preparation required to systematically defend OT/ICS networks running all public services across a nation is, of course, not a problem that can be adequately addressed solely through heightened awareness and training, security control frameworks, application of compliance standards or simply allocating enough budget, although any of these measures would help considerably to fill the gaps. However, a nation has to consider a much more cohesive approach to defending its CNIs. With the absence of a common strategy and unified vision enabled by clear lines of action and supported through well understood frameworks it is not possible for a country to systematically improve its cyber defence across the nation. Funding, awareness and misaligned efforts alone could fuel chaos and cause a waste of resources as everyone may try to solve the problem through their own particular means and methods. This, combined with a general lack of expertise in how to defend CNIs or ICS and OT environments, has amplified the issue.

3.4 Talent Gap

Despite the fact that the industry has been encouraging newcomers through a variety of initiatives, the cyber security talent pool has always been small. Below are some noteworthy initiatives that seek to address this challenge. However, there has not been any significant increase in the workforce to date and this thesis notes that the talent pool shortage is a global issue that is hereby acknowledged but not analysed in detail:

1. **Partnership Initiatives**[xv]: A partnership involving vocational education provider Te Pūkenga, Microsoft, TupuToa, and Te Whatu Ora Health New Zealand has been formed to address the need for skilled cybersecurity experts in New Zealand. This initiative aims to develop a micro-credential in cybersecurity to be offered from March 2023, focusing on providing on-campus and work-based experience. This program is particularly targeted at boosting diversity in the cybersecurity field and includes Microsoft certifications, which are highly sought after by employers. The growth in cybersecurity roles in New Zealand has been significant (65%), but there hasn't been a corresponding increase in the number of people with cybersecurity skills.
2. **Workforce Shortage and Skills Gaps**[xvi]: According to a report by ISC2, there is a significant cybersecurity workforce shortage globally, reaching nearly 4 million. This shortage is not just about the number of workers but also about the skills gap

in the cybersecurity profession. Key skills gaps include cloud computing security, AI/ML, and zero-trust implementation. Around 43% of cybersecurity workers cited significant or critical skills gaps within their companies. The report also highlighted the importance of investing in training and providing flexible working conditions to tackle these shortages.

3. **Government Initiatives (outdated)**[xvii]: In 2016, the New Zealand government established a Cyber Security Skills Taskforce, focusing on increasing the number of cyber professionals and developing a level 6 course with industry-supported internships. This task force was a response to the growing global shortage of cybersecurity professionals and the recognition that New Zealand is competing for talent in a global market. The task force included representatives from academia and industry to ensure that the training meets industry needs. No significant published outcomes of the task force's efforts were available to examine.
4. **Industry Challenges**[xviii]: An Information Systems Audit and Control Association (ISACA) survey in 2021 revealed that New Zealand and Australian cybersecurity teams are understaffed compared to the global average, with higher percentages of unfulfilled cybersecurity positions and applicants not being well qualified. The report further suggests that the tech sector in Australia and New Zealand is struggling to fill gaps in the cybersecurity talent market.

With a talent shortage and a deficit of almost 4 million people in the cyber security workforce globally, the challenge for CNIs and especially OT/ICS operators is even more pressing. Not all cyber security experts possess the skills and expertise to defend OT and ICS environments effectively as this requires further knowledge and specialisation to protect electric grids, water purification systems, food, and manufacturing industries. A detailed report from the World Economic Forum[xix] titled *Global Cyber Security Outlook 2023* provides further insights on the scale of the talent issue globally. Some key facts noted in the report are:

- the cyber security workforce needs to grow by 65% to effectively defend organisations' critical assets.
- 57% of organisations report that the cybersecurity skill shortage has a direct and high impact on them.
- there is a focus on recruiting from diverse backgrounds, but women still make up only 25% of the cybersecurity workforce.

In view of the foregoing global circumstances, it follows naturally that within New Zealand there are a limited number of cyber security professionals who have well-rounded exposure and experience with the latest technology platforms, cloud services, and OT/ICS environments combined.

3.5 Disconnected Strategies

In August 2023, the New Zealand Ministry of Defence released its policy and strategy statement for 2023[xx] highlighting initiatives to be undertaken by New Zealand as a nation in the fields of planning, operations, engagement, and investments so as to ensure that its lines of defence are fit-for-purpose in an increasingly challenging and complex world. This statement acknowledges that New Zealand's defence works alongside other agencies to protect against a range of security threats, including ensuring the nation's authority and freedom of action across broader domains such as sea, air, space, and importantly, cyber lines of communication. This indicates a recognition of the importance of digital security and the need to safeguard against cyber threats as part of the nation's overall defence strategy. It does perceive cyber threats as a significant component of the broader security challenges. The document emphasises the importance of understanding and actively shaping the security environment, which implicitly includes addressing cyber threats, which are seen as an element of the complex and evolving security challenges that New Zealand faces, particularly in the context of its strategic environment and relationships with its allies. However, the statement does not refer to any directly linked lines of actions or adoption of proactive and purposeful actions to improve cyber security of the CNIs in the nation.

At approximately the same time as the release of the above-mentioned statement in August 2023, the New Zealand Government released the *National Security Strategy for Aotearoa New Zealand*[xxi] with the following vision. (DPMC New Zealand , 2023)"...At the heart of our national security approach is a whole-of-society vision: A secure and resilient Aotearoa New Zealand—one that is protected as a free, open, and democratic society for future generations…". The document outlines New Zealand's approach to national security, emphasizing the need for a secure, resilient society. It focuses on protecting against various threats, including strategic competition, cyber security, and terrorism, with a strong emphasis on working together both domestically and internationally. The strategy incorporates lessons from past events and recognizes the interconnected nature of global

and local security challenges, aiming for early threat detection and fostering resilience within the community and across government sectors. It emphasises the growing threat from malicious cyber actors, including state and non-state actors. It notes that the government has taken steps to enhance New Zealand's cyber security capability since the Cyber Security Strategy 2019, focusing on protecting data, networked devices, and infrastructure and outlines future plans, including strengthening cyber resilience of critical infrastructure, improving cyber incident reporting, fostering government-industry collaboration, and expanding the Government Communications Security Bureau's (GCSB) threat detection and disruption services. The strategy outlined in the document for enhancing cyber security in New Zealand includes:

1. **Strengthening Cyber Resilience of Critical Infrastructure**: Implementing measures to enhance the security and resilience of infrastructure essential to national security and economy.
2. **Improving Cyber Incident Reporting Mechanisms**: Developing more efficient systems for reporting and responding to cyber incidents, enabling timely and effective mitigation.
3. **Enhancing Access to Information and Support**: Providing better access to resources and support for organisations and individuals to defend against cyber threats.
4. **Increasing Collaboration between Government and Industry**: Fostering partnerships between government entities and private sector to share knowledge, resources, and strategies for cyber defence.
5. **Expanding GCSB's Threat Detection and Disruption Services**: Enhancing the capabilities of the Government Communications Security Bureau to detect and counter sophisticated cyber threats, both for government and private sector entities.

In December 2023, the New Zealand National Cyber Security Centre (NCSC) released a document titled *Strategy to 2024*[xxii] which articulates an approach to improving cyber defence in general and reflects on some upcoming and in-progress changes announced earlier during the year in August[xxiii] to create a lead operational cyber security agency. However, this still did not focus explicitly on the protection of CNIs or organisations operating OT and ICS environments to provide critical services.

With recent cyber-attacks impacting New Zealand's critical services and its citizens, alongside the increasing complexity of the cyber security landscape, a stark increase in new vulnerabilities discovered in OT/ICS systems, the increased motivations of cyber attackers - both nation-state and cybercriminal entities - and evidence of an increased frequency of cyber-attacks on CNIs across the globe - the above government publications and initiatives clearly acknowledge the need for improvements and highlight the requirement for a systematic, concentrated, and collaborative effort to combat the challenges for New Zealand as a nation. However, owing to the lack of a unified vision and clear strategies supported by well-defined lines of actions, there have been no significant advancements in defending critical infrastructure within the current threat landscape.

The goal of this thesis is to identify potential shortcomings and areas for enhancement in New Zealand's cybersecurity approaches, so as to highlight specific lines of actions in the form of hypotheses to support strategic improvements to defend the CNIs where OT and ICS are employed. Learnings from this thesis may be used for academic and pragmatic application of hypotheses in consultations and considerations by policy makers, cyber security leaders and the government of New Zealand, when considering lines of actions to enhance the current state of how critical national infrastructure in New Zealand is defended.

4 Scope and Methodology

4.1 Scope

This thesis focuses on enhancing protection from cyber threats for critical national infrastructure services operating OT and ICS environments and providing critical services to the people of Aotearoa New Zealand. The objective of the thesis is to highlight current shortcomings and issues in the cyber defence approach employed by the government and industry in New Zealand in its efforts to defend these systems as the threat landscape evolves. Through literature review, the researcher's own exposure and learning within the field, and expert interviews, this thesis provides a subjective analysis of current gaps and outlines hypotheses to be taken into consideration when defining the future strategy. This thesis does not attempt to provide a roadmap for the implementation of any of the hypotheses or rate the severity of any shortcomings and issues identified through expert interviews and literature review, as attempting to prioritize and develop a roadmap or lines of actions in the absence of a clear strategy will be premature. Consequently, this thesis is limited to providing hypotheses for the consideration of relevant audiences within the New Zealand government and CNI organisations across the nation.

Additionally, the thesis will not consider:

- Specific Technical Solutions: The thesis will not delve into detailed technical cybersecurity solutions or technologies; rather, it will focus on approaches, frameworks, and standards.
- Non-CNI Sectors: The analysis is confined to CNIs and does not extend to cybersecurity practices in non-CNI sectors.
- Immediate Operational Changes: The research aims at strategic and policy-level implications rather than immediate operational changes within organisations.
- Non-Cybersecurity Related Aspects of CNIs: Aspects of CNIs unrelated to cybersecurity, such as physical security or economic considerations, are not within the purview of this study.

4.2 Research Methodology

The research methodology for this thesis was structured as follows:

Table 3: Research Methodology

Phase	Objective	Approach
Comprehensive Literature Review and Framework Identification	To systematically identify and collate current approaches, strategic direction and relevant government-enforced frameworks and definitions related to ICS/OT cybersecurity within the Five Eyes (Five Eyes) nations.	This was accomplished through an extensive literature review encompassing academic policies, industry reports, and official government publications. Additionally, a thorough examination of government websites of Five Eyes nations was conducted to extract pertinent cybersecurity frameworks.
Comparative Analysis of Cybersecurity Standards	To analyse the current state of cybersecurity standards implemented within CNIs operating ICS/OT environments, with a specific focus on the requirements enforced by the Government of New Zealand.	The identified practices from other Five Eyes nations were analysed to elucidate their purpose, scope, and specific benefit. This analysis incorporated an assessment of the strengths of these frameworks, followed by a comparative evaluation against the cybersecurity standards practiced in New Zealand.
Survey Development and Implementation	To develop and administer a survey aimed at assessing the perceived efficacy of current cybersecurity standards among various CNI organisations in New Zealand.	The survey was meticulously crafted to gather insights on the experts' comprehension of, compliance with, and challenges faced in implementing good practices and frameworks. It was also designed to probe the impact of the absence of standardised cybersecurity measures in New Zealand, along with soliciting open opinions of experts on the current state and future strategy to gather information for subjective analysis.
Survey Distribution and Data Collection	To disseminate the survey across a representative cross-section of CNI organisations operating ICS/OT environments in New Zealand.	The survey was distributed through multiple channels, including online platforms and direct mail to ensure a comprehensive reach and robust response rate. The survey was conducted through video calls between the experts and the researcher directly to foster candid

Phase	Objective	Approach
		conversation and open data collection.
Protection of privacy and ethics considerations	To ensure protection of privacy of information for all experts involved in the survey while collecting meaningful data with their consent only.	The thesis followed the ethics approval process outlined by the Waikato University and defined measures such as not collecting or using any unnecessary private information about those surveyed or contacted experts beyond contact details used for distribution and not recording video calls or audio from any of the surveys conducted. No organisation or experts are quoted or named during the analysis.
Data Analysis and Interpretation	To analyse the collected survey data for insights into the subjective perspectives on the effectiveness, challenges, and compliance levels regarding cybersecurity frameworks and standards.	Statistical techniques were employed to interpret the survey data, aiming to uncover trends, correlations, and patterns that reveal the experts' stance on current cybersecurity practices.
Formulation of Observations and Hypotheses	To synthesize observations and formulate hypotheses aimed at enhancing the current cybersecurity landscape for CNIs in New Zealand.	This stage involved integrating the findings from the literature review analysis and field survey data to develop informed observations. These observations were then used to construct hypotheses that propose potential improvements and strategies for bolstering cybersecurity for CNIs operating ICS/OT environments within New Zealand.

This methodology was designed to ensure a rigorous, comprehensive, and systematic approach to understanding and improving the cyber defence mechanisms of ICS/OT environments in New Zealand's CNI sector.

The following sections outline the analysis of the literature review and field study through surveys, followed by outlining hypotheses as noted above.

5 Literature Review and Landscape Analysis

5.1 Approach to analysis

Each of the five eyes nations (Australia, Canada, New Zealand, UK and USA) defines CNI in ways that reflect their national priorities and security concerns. However, these definitions are not entirely consistent across these countries, leading to some discrepancies in what is considered critical infrastructure. Following is a summary of how each country defines CNI and some notable inconsistencies:

5.1.1 Definition of CNI

Following is a brief outline of how each of the five eyes nations define their CNI and some of the principles or approaches each consider in the definition:

1. **United States**:
    - CNI is defined through the Department of Homeland Security (DHS) as sectors vital to ensuring national security, economic health, and public safety. These sectors include energy, water, transportation, communications, and others.[xxiv]
    - The USA has a broad and inclusive approach, encompassing a wide range of sectors.

2. **United Kingdom**:
    - The UK identifies 13 national infrastructure sectors, which include Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport, and Water.[xxv]
    - The UK's approach is quite comprehensive but less focused on technology infrastructure and interconnectedness of CNIs as compared to the USA.

3. **Canada**:
    - Canada's approach to defining CNI is similar to that of the USA and UK, focusing on systems and assets critical to national security, health, safety,

economic prosperity, or public confidence. Canada's emergency management framework sets out the need for the protection of ten (10) critical infrastructure sectors.[xxvi]

- Canada includes a unique emphasis on public confidence, which is not explicitly mentioned in the other Five Eyes definitions.

4. **Australia**:

    - Australia identifies CNI as physical facilities, supply chains, information technologies, utilities, and communications networks crucial for the nation's functioning. The latest amendments to Australia's Security of Critical Infrastructure Act 2018 (SOCI) further expand on this definition and provides clearer guidance on security requirements to protection CNI. [xxvii]
    - The Australian definition is distinctive in its explicit emphasis on services that are essential for everyday life such as energy, food, water, transport, communications, health and banking and finance.

5. **New Zealand**:

    - New Zealand's definition of CNI is less specific than the other Five Eyes countries and focuses on systems and assets essential to the national security and economic well-being. New Zealand is in the beginning of defining the critical infrastructure within the context of emergency management for a more resilient and well-governed nation.[xxviii]
    - New Zealand's approach appears more fluid and less detailed, potentially leading to a broader interpretation.

5.1.2 Inconsistencies

Following is an outline of some of the key inconsistencies that are highlighted throughout this thesis:

- **Scope and Specificity**: The USA and UK have broader and more technology-focused definitions based on how CNIs are interconnected, whereas Australia and Canada have more traditional and slightly narrower

scopes. New Zealand, however, has not defined the scope of CNI and considers it a priority to do so, within 2023.

- **Public Confidence**: Canada's unique emphasis on public confidence as a criterion is not explicitly found in other nations' definitions.
- **Technological Emphasis**: Australia's specific mention of information technologies and supply chains shows a more modernised approach, which is less explicit in other countries, including New Zealand.
- **Fluidity**: New Zealand's less detailed approach can lead to a more fluid interpretation of what constitutes CNI, as opposed to the more specific sectors listed by countries like the USA and UK.

5.1.3 Framework for the Analysis

Obviously, it would have been challenging to carry out any close comparative and subjective analysis and literature review based on just the definition of CNI and how OT and ICS assets are protected in each country. Therefore, for the purpose of depicting cyber security preparedness, this thesis considered certain attributes to be important for a nation to be able to defend CNI effectively (this, by the very nature of CNI, includes defence for OT and ICS networks). This thesis uses a unique framework for analysis beyond simply cyber security standards or baseline security controls as these attributes include capabilities and approaches a nation must consider in defending CNIs comprehensively and having a sustainable model for cybersecurity preparedness in place to evolve as the threat landscape changes.

There is currently no global standard framework available for assessing the maturity of nations to protect their most critical assets and services from cyber-attacks. There are maturity assessment frameworks such as C2M2 [xxix], used by many industries and organisations around the world. However, C2M2 and other such maturity models are designed to assess the coverage and effectiveness of specific controls and standards. This approach may be effective when it comes to establishing and operating a cyber security program for an organisation or an industry. However, when it comes to assessing a nation's capability to defend its critical infrastructure and to sustain that capability as the threat landscape evolves, adherence to standards alone will not suffice. Therefore, this thesis presents a unique framework to examine ten (10) attributes for two (2) capability pillars to analyse the ability of a nation to defend its CNI and maintain a strong culture and posture

of cyber defence supported through proactive and collaborative lines of actions. This framework for analysis is used throughout the thesis and is referred to as CNI Cyber Defence Maturity Framework (CCDM) hereon. Following is a list of attributes considered within the CCDM for subjective analysis:

5.1.3.1 Cyber Defence of Critical Infrastructure

This assesses a nation's ability to protect its critical infrastructure against cyber threats. Key attributes include:

1. **Definition of CNI and Security Measures**: How CNIs are defined, and the robustness of cybersecurity measures implemented specifically for critical infrastructure.
2. **Incident Response for CNI**: Effectiveness of strategies and protocols for responding to cyber incidents that have an impact on critical infrastructure.
3. **Investment in CNI Protection**: Financial and resource allocation towards safeguarding critical systems.
4. **Public-Private Partnerships in CNI Defence**: The extent and effectiveness of collaboration between government agencies and private sector entities managing CNI.
5. **Regulatory Compliance for CNI Security**: Stringency and enforcement of laws and regulations governing CNI cybersecurity.

5.1.3.2 Cybersecurity Preparedness

This dimension evaluates the overall readiness and sustainability model of a nation’s ability to handle and mitigate cyber threats as they evolve. Considered attributes are:

1. **National Cybersecurity Strategy**: The existence and comprehensiveness of a national strategy dedicated to cybersecurity.
2. **Workforce Development and Expertise**: The level of skill and the size of the workforce dedicated to cybersecurity.
3. **Technological Advancement in Cybersecurity**: The use of cutting-edge technologies for cyber defence.
4. **Threat Intelligence and Information Sharing**: Capability to gather, analyse, and share cyber threat intelligence.
5. **Public Awareness and Education**: Efforts to educate the public and raise awareness about cybersecurity.

5.2 Detailed Analysis

Upon examining publicly available policies, government strategies, and approaches employed across the Five Eyes countries, this thesis highlights the following key insights regarding approaches taken by each of the countries for each of the attributes examined that contribute to the subjective analysis. For this thesis a comparative analysis of all five eyes counties revealed some useful insights in understanding how each nation defines and protects its CNI. The author has intentionally highlighted a deeper level of detail for New Zealand and Australia from the five eyes countries due to geographic, cultural and threat landscape similarities the two nations share. Additionally, Estonia and Singapore were added to the analysis as these two nations offer insights based on recent learnings from significant investments in their CNI cyber defence and because they also share some characteristics with New Zealand, highlighted below within this section.

5.2.1 New Zealand

The New Zealand Government Communications Security Bureau (GCSB) oversees the operation of the Nation Cyber Security Centre in New Zealand (NCSC NZ), and its objectives are to detect, disrupt, and deter high-impact cyber threats, and to deliver preventative advice and support to nationally significant organisations. There is no clear definition of "nationally significant organisations" outlined on by the NCSC[xxx] or in GCSB published guidelines.

Currently, the New Zealand government has published a report titled *Defence Policy and Strategy Statement 2023*[xxxi], which acknowledges cyber threats as a priority area of focus. GCSB has published a "New Zealand's National Security Strategy 2023-2028"[xxxii] and NCSC has published a *Strategy to 2024*[xxxiii].

None of the above strategies highlight detailed definitions of nationally significant organisations or critical national infrastructure organisations and neither outlines direct strategies and lines of actions for the protection of CNIs or organisations operating OT and ICS environments. The only well-known and adopted set of guidelines by government agencies in New Zealand is the New Zealand Information Security Manual (NZISM), which is considered an integral part of the Protective Security Requirements (PSR) framework which sets out the New Zealand Government's expectations for the management of personnel, information and physical security as directed by Cabinet[xxxiv]. NZISM is a national standard adopted by the government agencies as a measure of

assurance against a baseline, but there is no enforcement of any such standard for critical national infrastructure organisations in the private sector when it comes to cyber security or information security requirements. The only noteworthy security risk framework which applies as a legislative requirement relates to the Telecommunications sector with respect to the Telecommunications (Interception Capability and Security) Act (TICSA)[xxxv]. This, however, is only in the context of telecommunications networks and their impact on national security and is intended to allow facilitation of Interception Capability and Security to maintain order and safety. There exists a voluntary cyber security standard developed specifically by the representatives of the energy sector in New Zealand in collaboration with the NCSC.[xxxvi] However, this remains voluntary and continues to be a work in progress with no tangible outcomes thus far to significantly advance security controls for the industry. NCSC also advertises a few resources[xxxvii], mainly external, from within Five Eyes countries as guidelines for ICS cyber security. None of these resources provide specific guidance that is explicitly applicable to NZ CNI service providers.

In light of the above, any organisation operating OT and ICS assets and systems and providing critical services to NZ citizens can choose to adhere to NZISM or any other industry standard and maintain a level of maturity suitable for its business risk tolerance. There are no mandatory reporting, or assessment, or information sharing agreements in place for most, if not all, CNI sectors when it comes to maintaining and operating cyber security of critical services.

Below are two additional noteworthy NZ government initiatives that this thesis considered:

5. **Emergency Management Bill**: The "Emergency Management Bill" of New Zealand[xxxviii] includes provisions for critical infrastructure protection, emphasizing the improvement of resilience before, during, and after emergencies. Specifically, it outlines obligations for critical infrastructure entities, such as sharing information with relevant agencies and establishing emergency service levels. The bill focuses on clarifying roles and responsibilities within the emergency management system, including those of local government and critical infrastructure providers. However, it does not explicitly note any provisions for OT or ICS asset protection. The bill does, nonetheless, represent a promising development because, for the provisions of this bill to come into effect, New Zealand will be required to define “critical infrastructure entities” and categorise these entities based on emergency service

levels. There was no evidence of how the outcome of this bill and the provisions noted therein will align or interact with the cyber security strategy and ongoing initiatives.

6. **Consultation on strengthening the resilience of Aotearoa New Zealand's critical infrastructure system** [xxxix] : this discussion paper, prepared for the consultation facilitated by the Department of the Prime Minister and Cabinet (DPMC), explicitly acknowledges the convergence of Operational Technology (OT) and Information Technology (IT) systems as a significant challenge to infrastructure resilience. This convergence expands the attack surface and exposes critical systems to new vulnerabilities, where malicious actors can gain access to systems that monitor and control physical equipment, potentially leading to the disruption or disablement of operations. This recognition of the vulnerabilities in the integration of OT and IT systems is crucial for New Zealand's defence of Critical National Infrastructures (CNIs). By identifying these challenges, New Zealand can focus on developing strategies and measures specifically tailored to protect OT and ICS assets. These assets are integral to the functioning of many critical infrastructures, including utilities, transportation, and healthcare systems.

The emphasis on the risks posed by the integration of OT and IT highlights the need for:

- Enhanced cybersecurity measures that address both digital and physical threats.
- Specialised training and development of workforce skills to manage and secure these integrated systems.
- Development and implementation of robust incident response protocols specifically for OT and ICS environments.
- Strengthening public-private partnerships to ensure comprehensive coverage and protection of these critical systems.

Following is the analysis based on CCDM for New Zealand:

5.2.1.1 Cyber Defence of Critical Infrastructure

New Zealand's approach to protecting its critical national infrastructure (CNI) against cyber threats is fluid and is currently under development, involving various strategies which still require further alignment and collaboration.

1. **Definition of CNI and Security Measures:** The New Zealand Lifelines Council released the 2023 Edition of the report titled *New Zealand Critical Infrastructure*[xl]*: A National Vulnerability Assessment*. This assessment provides insights into the vulnerabilities of New Zealand's critical infrastructure, aiming to enhance the understanding of risks and the need for robust security measures.

2. **Incident Response for CNI:** The National Cyber Security Centre (NCSC) of New Zealand plays a pivotal role in incident response. The NCSC's 2022/2023 Cyber Threat Report highlights the increasing and deepening partnerships that offer unprecedented threat protection, with millions of New Zealanders now benefiting from the Malware Free Network (MFN) threat detection and disruption service.[xli] There is, however, no mandatory reporting and therefore it remains unknown to what degree NZ is impacted by threats within the CNI and whether the government, through NCSC and CERT NZ, is capable of responding to impactful security incidents effectively.

3. **Investment in CNI Protection:** There is no clear and recent messaging about a tangible investment for CNI specific improvements. However, New Zealand's *Defence Assessment 2021* and *Cyber Security Strategy 2019* emphasise the importance of state-sponsored cyber operations and the corresponding need to increase the frequency of such events. This highlights the country's investment in understanding and defending against these sophisticated threats.[xlii]

4. **Public-Private Partnerships in CNI Defence:** There is a recognition of the need for collaboration between government and private sectors in containing cyber risks. This includes efforts aimed at protecting operational technology (OT) systems and aging critical infrastructure, as well as enhancing the resilience of these systems against cyberattacks and other forms of interference.[xliii]

5. **Regulatory Compliance for CNI Security:** New Zealand is focused on improving the security of cloud services and reducing risks associated with rapid technology deployment. Efforts include implementing formal sign-off processes, creating DevSecOps workflows, and limiting access to cloud environments to mitigate risks. These are in-progress and planned initiatives, but no tangible plans for implementation or a strategy to make changes in a gradual manner are publicly available. [xliv]

5.2.1.2 Cybersecurity Preparedness

New Zealand's cybersecurity preparedness involves a mix of ongoing efforts and measures, strategic frameworks, and collaborative efforts to build a resilient digital environment.

1. **National Cybersecurity Strategy:** There is no single strategy that outlines the approach to defending against state-sponsored and criminal cyber activities, emphasizing the importance of protecting critical systems and democratic processes from cyber threats. Various efforts are currently in progress as noted in the analysis above.

2. **Workforce Development and Expertise:** The NCSC's efforts to expand its threat detection services and its collaboration with private sector partners indicate a commitment to developing cybersecurity expertise and a corresponding workforce within the country.

3. **Technological Advancement in Cybersecurity:** The expansion of threat detection services and the focus on modernizing cybersecurity tools reflect New Zealand's commitment to using advanced technologies in cyber defence.

4. **Threat Intelligence and Information Sharing:** The NCSC's collaboration with domestic and international agencies enhances the country's capability in threat intelligence and information sharing, which are crucial for understanding and mitigating cyber threats.

5. **Public Awareness and Education:** New Zealand's current emphasis on developing comprehensive cybersecurity strategies, which includes. holding public consultations on this important topic and collaboration between government and industry underline the importance of public awareness and education in cybersecurity.

5.2.2 Australia

The Security Legislation Amendment (*Critical Infrastructure Protection*) Bill[xlv] is a central component of Australia's strategy. This legislation enhances the security and resilience of critical infrastructure against various threats, including cyber-attacks. It requires infrastructure owners and operators to manage risks that could impact the delivery of essential services. This approach is aligned with Australia's Cyber Security Strategy 2020

and is part of the government's broader efforts to strengthen the management of and response to security risks across critical infrastructure sectors.

The Australian Cyber Security Strategy for 2023-2030[xlvi] represents a comprehensive approach to enhancing national cyber resilience and security. It focuses on a range of key areas, including protecting critical infrastructure, providing businesses and organisations with tools to bolster cyber resilience (especially against ransomware attacks), ensuring secure products and services, attracting skilled migrants for a diverse cyber security workforce, prioritizing critical threats, engaging international partners for threat intelligence and capability development, and expanding cyber awareness programs. This strategy is supported by a significant investment of $586.9 million, in addition to $2.3 billion committed to existing cyber initiatives.

The strategy outlines six main "shields" for cyber defence: strengthening businesses and citizens, ensuring safe technology, world-class threat sharing and blocking, protecting critical infrastructure, building sovereign capabilities, and fostering resilient regional and global leadership. Each of these shields encompasses various actions and resource allocations, highlighting Australia's commitment to becoming a world leader in cyber security by 2030.

Compared to New Zealand's approach, Australia's strategy is more detailed in terms of specific actions, funding allocations, and the establishment of collaborative frameworks between government, industry, and international partners. Notably, Australia's focus includes a wide range of sectors, emphasizing the need for strengthened critical infrastructure and a concerted effort to enhance the cyber resilience of businesses and citizens. Additionally, Australia places significant emphasis on international cooperation and regional leadership in cyber security.

In contrast, New Zealand's strategy, while comprehensive, appears less detailed in terms of specific actions and resource allocations. New Zealand's approach focuses on strengthening cyber resilience, improving incident reporting, enhancing information access, fostering government-industry collaboration, and expanding GCSB's capabilities. However, it lacks the specific funding allocations and detailed action plans found in Australia's strategy.

Overall, the noteworthy gaps in New Zealand's strategy compared to Australia's include less detailed information on funding allocations, specific sector-focused actions, and the depth of the international collaboration and capacity-building efforts that Australia seeks to pursue. Australia's strategy presents a more targeted and resource-specific approach, emphasizing a broader range of sectors and detailed plans for enhancing cyber security at various levels.

5.2.2.1 Cyber Defence of Critical Infrastructure

Australia has implemented a comprehensive approach to protecting its critical national infrastructure (CNI) from cyber threats, which includes legislative reforms, technological innovations, and strategic partnerships.

1. **Definition of CNI and Security Measures:** The Australian Government released the *2023-2030 Australian Cyber Security Strategy* which is aimed at making Australia a world leader in cyber security by 2030 and includes six cyber shields to protect against threats. These shields focus on strengthening businesses and citizens, ensuring safe technology, world-class threat sharing and blocking, protecting critical infrastructure, developing sovereign capabilities, and fostering resilient regional and global leadership.[xlvii]

2. **Incident Response for CNI:** The Australian Government has been proactive in responding to increasing cyber threats to critical infrastructure. In response to the growing threat, enhanced cybersecurity measures have been announced for 168 critical infrastructure assets, almost double the number previously identified as 'systems of national significance'. This, combined with clear guidance with SOCI Act amendment and the efforts to make it easier to report incidents through dedicated hotline and advisory support through the Australian Signals Directorate (ASD)’s and the Australian Cyber Security Centre (ACSC) shows a strong commitment from the Australian government. [xlviii]

3. **Investment in CNI Protection:** As an element of its cyber security strategy, the Australian Government plans to implement key initiatives across the government over the next two years. This includes addressing critical gaps in Australia's cyber shields and building strong partnerships across industry and government.[xlix]

4. **Public-Private Partnerships in CNI Defence:** A notable example of innovation in cybersecurity is the collaboration between the Royal Melbourne Institute of Technology [RMIT University] and the Tide Foundation. They have developed ‘ineffable cryptography’, which is a new technology for critical infrastructure management, which allows system access authority to be spread invisibly and securely across a network, reducing the risk of hacking.[l]

5. **Regulatory Compliance for CNI Security:** The *Security of Critical Infrastructure Act 2018* has been amended to include obligations to report cyber security incidents and to implement a risk management program. These amendments provide a framework for managing and protecting critical infrastructure, including government information gathering, direction, and intervention powers.[li]

5.2.2.2 Cybersecurity Preparedness

Australia's cybersecurity preparedness strategy includes a combination of legislative measures, technological advancements, and collaborative efforts.

1. **National Cybersecurity Strategy:** The *2023-2030 Australian Cyber Security Strategy* outlines a roadmap for achieving a secure digital ecosystem and becoming a global leader in cybersecurity by 2030. It emphasises the importance of collaboration and partnership to tackle cyber problems.

2. **Workforce Development and Expertise:** The collaboration between RMIT University and the Tide Foundation, along with other industry partnerships, shows a focus on developing cybersecurity expertise and innovative solutions.

3. **Technological Advancement in Cybersecurity:** The development of new technologies such as ineffable cryptography demonstrates Australia's commitment to advancing cybersecurity technologies to protect against sophisticated cyber threats.

4. **Threat Intelligence and Information Sharing:** The cybersecurity strategy includes a focus on world-class threat sharing and blocking, indicating a strong commitment to intelligence gathering and information sharing to combat cyber threats.

5. **Public Awareness and Education:** The strategy's focus on supporting citizens and businesses in managing cyber risks highlights the importance of public awareness

and education in cybersecurity. Another impactful decision Australian government made in 2022 is to appoint a minister for cyber security.

5.2.3 Canada

Canada's approach to protecting its critical national infrastructure (CNI) against cyber threats involves a coordinated effort by various government entities and collaboration with academia and industry. Canada generally aligns with USA when it comes to cyber defence for critical infrastructure because the two countries share natural resources as well infrastructure, such as the supply of electricity and using hydro infrastructure for electricity generation. The North American Electric Reliability Corporation (NERC) was established in recognition of this shared threat landscape and interdependency.

5.2.3.1 Cyber Defence of Critical Infrastructure

1. **Definition of CNI and Security Measures:** Canada's *National Cyber Threat Assessment 2023-2024* highlights the evolving nature of cyber threats faced by individuals, organisations, and critical infrastructure providers. The report emphasises the need for robust cybersecurity measures to protect against threats such as ransomware, which is considered the most disruptive form of cybercrime in Canada. The government emphasises safeguarding critical infrastructure from these evolving threats through various programs and initiatives.[lii]

2. **Incident Response for CNI:** The Canadian Centre for Cyber Security, part of the Communications Security Establishment[liii], is at the forefront of incident response. It collaborates with businesses and organisations victimised by cyber incidents to mitigate their impacts. The Centre provides expert advice, guidance, services, and support on cyber security operational matters, playing a critical role in defending against and responding to cyber threats.

3. **Investment in CNI Protection:** The Government of Canada has made significant investments in cybersecurity, including a provision of $144.9 million in Budget 2019 to introduce a new critical cyber systems framework for federally regulated critical infrastructure sectors such as finance, telecommunications, energy, and transport. Additionally, $875 million over five years, and $238 million ongoing, to enhance Canada's cybersecurity capabilities.[liv]

4. **Public-Private Partnerships in CNI Defence:** Canada has emphasised the importance of collaboration with industry and academia to enhance cybersecurity. Notably, new funding for innovative cybersecurity projects at the Université de Sherbrooke aims to enhance critical infrastructure protection, focusing on the resilience of the electrical grid and cybersecurity in 5G connectivity.[lv]

5. **Regulatory Compliance for CNI Security:** The introduction of Bill C-26, *An Act Respecting Cyber Security* (ARCS), marks a significant step in strengthening Canada's cybersecurity. This legislation aims to bolster cybersecurity across key sectors and introduces the *Critical Cyber Systems Protection Act* (CCSPA) to secure Canada's critical infrastructure.[lvi]

5.2.3.2 Cybersecurity Preparedness

Canada's preparedness for cybersecurity threats involves a comprehensive approach, with an emphasis on understanding and mitigating various cyber threats.

1. **National Cybersecurity Strategy:** The *National Cyber Threat Assessment* and other government publications provide insights into the cyber threats facing the country and outline Canada's strategic approach to cybersecurity.

2. **Workforce Development and Expertise:** The government's collaboration with academic institutions such as the Université de Sherbrooke indicates a focus on developing cybersecurity expertise and a corresponding workforce.

3. **Technological Advancement in Cybersecurity:** Investments in cybersecurity, as outlined in recent budgets, reflect Canada's commitment to using advanced technology to combat cyber threats.

4. **Threat Intelligence and Information Sharing:** The Canadian Centre for Cyber Security plays a pivotal role in gathering and sharing cyber threat intelligence, aiding in national and international cybersecurity efforts.

5. **Public Awareness and Education:** The government's emphasis on cybersecurity in public statements and its collaborations with academic institutions highlight the importance it places on public awareness and education in this domain.

5.2.4 United Kingdom

The UK's approach to protecting its critical national infrastructure (CNI) against cyber threats is multi-faceted and robust, involving a combination of government initiatives, regulations, and public-private partnerships.

5.2.4.1 Cyber Defence of Critical Infrastructure

1. **Definition of CNI and Security Measures:** The UK has implemented the Network and Information Systems Regulations (NIS Regulations), designed to safeguard critical infrastructure from cyberattacks. These regulations mandate technical and organisational measures to ensure robust cybersecurity across the country's critical infrastructure, including regular vulnerability tests and new systems for quick detection and response to cyberattacks.[lvii]

2. **Incident Response for CNI:** The National Cyber Security Centre (NCSC), part of GCHQ, plays a critical role in coordinating incident response efforts for CNI. The NCSC has recently issued warnings about heightened threats to UK critical infrastructure and services, especially from Russia-aligned cyber attackers. These alerts emphasise the need for urgent steps to increase cyber security resilience.[lviii]

3. **Investment in CNI Protection:** The UK government is committed to investing in both public and private sector measures to improve the nation's cybersecurity posture. This includes collaborations with industry stakeholders, universities, and research institutes to develop new cybersecurity technologies. In its Government *Cyber Security Strategy 2022–2030*, the UK government committed to a budget of over 37 million GBP for cyber security within the period of the plan. The majority of this budget is dedicated to defending CNIs within the UK.[lix]

4. **Public-Private Partnerships in CNI Defence:** The UK government and the NCSC work closely with private sector CNI operators to ensure adequate levels of resilience across all sectors. By 2025, CNI organisations will have specific resilience targets to meet, underlining the collaborative approach to cybersecurity.[lx]

5. **Regulatory Compliance for CNI Security:** In addition to the NIS Regulations, UK organisations must comply with the NCSC's Cyber Essentials certification program, which sets a baseline for cybersecurity measures. Organisations are also required to report any security incidents to the government. [lxi]

5.2.4.2 Cybersecurity Preparedness

The UK faces a complex cyber threat environment, with challenges ranging from state-sponsored attacks to cybercrime, espionage operations, and financially impactful cyber-attacks, particularly ransomware.

7. **National Cybersecurity Strategy:** The UK's National Cyber Strategy focuses on countering these threats through a combination of sanctions against cybercriminals, strategic partnerships, and investment in cyber capabilities. The strategy is aligned with broader geopolitical considerations, such as the impacts of Russia's invasion of Ukraine.
8. **Workforce Development and Expertise:** The UK recognizes the skills gap in the cybersecurity sector and is working on diversifying and increasing the cyber workforce. There has been progress in increasing the representation of ethnic minorities and women in cybersecurity roles.
9. **Technological Advancement in Cybersecurity:** The UK is focused on keeping pace with technological developments in cybersecurity to compete with global powers and protect against sophisticated cyber tools and services.
10. **Threat Intelligence and Information Sharing:** There is an emphasis on forming international relationships and sharing attack data to build resilience. The UK is involved in shaping the international dialogue over the rules governing cyberspace, highlighting the importance of collective action in cyber defence.
11. **Public Awareness and Education:** Addressing the broader challenges in cybersecurity, the UK government emphasises the need for public and private sectors to be aware of and prepared for cyber threats. The focus is also on educating the workforce and the general public about cybersecurity best practices.

5.2.5 United States of America

With a strong focus on regulatory enforcements, leadership in the development of various standards such as the National Institute of Standards and Technology (NIST), and North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) for the energy sector, alongside leading agencies such as the Cybersecurity and Infrastructure Security Agency (CISA), the USA reflects its recognition of the need for

defending the CNIs in the complex threat landscape in which it operates and its commitment to implementing measures towards that end.

5.2.5.1 Cyber Defence of Critical Infrastructure

The United States has developed a comprehensive strategy for defending its CNI against cyber threats, underpinned by the National Cybersecurity Strategy and the efforts of various federal agencies.

1. **Definition of CNI and Security Measures:** The Biden-Harris Administration's *National Cybersecurity Strategy*, released in March 2023, aims to ensure a safe and secure digital ecosystem for all Americans. This strategy focuses on rebalancing the responsibility to defend cyberspace by shifting the burden from individuals, small businesses, and local governments to larger organisations better positioned to reduce risks. It also seeks to realign incentives, so as to favour long-term investments in cybersecurity, thereby enhancing the defence and resilience of the nation's critical infrastructure.[lxii]

2. **Incident Response for CNI:** The National Security Agency (NSA) plays a significant role in the United States' cybersecurity landscape. The NSA's *2023 Cybersecurity Year in Review* highlights its achievements in defending against global threats, establishing the Artificial Intelligence Security Centre, and detecting intrusions into U.S. critical infrastructure, particularly by state actors like China. These efforts underscore the agency's commitment to enhancing national security through cybersecurity.[lxiii]

3. **Investment in CNI Protection:** The Cybersecurity and Infrastructure Security Agency (CISA), established by Congress in 2018, is tasked with understanding, managing, and reducing risk to both cyber and physical critical infrastructure. CISA's strategic plan for 2023-2025 focuses on two key roles: ensuring the defence and resilience of cyberspace and reducing risks to critical infrastructure resilience and security.[lxiv]

4. **Public-Private Partnerships in CNI Defence:** The National Cybersecurity Strategy emphasises the importance of public-private collaboration in defending critical infrastructure and essential services. This includes expanding the use of

minimum cybersecurity requirements in critical sectors and enabling collaboration at the necessary speed and scale.[lxv]

5. **Regulatory Compliance for CNI Security:** The strategy also acknowledges the need for harmonizing regulations to reduce compliance burdens while ensuring national security and public safety. This approach aligns with efforts to modernize Federal networks and update Federal cybersecurity measures.[lxvi]

5.2.5.2 Cybersecurity Preparedness

The United States' approach to cybersecurity preparedness involves a multi-faceted strategy that includes strengthening cybersecurity foundations, addressing critical gaps, and building robust partnerships across industry and government.

1. **National Cybersecurity Strategy:** The National Cybersecurity Strategy is a game-changer for the United States, shifting cybersecurity from a technical topic to a whole-of-nation endeavour. It focuses on better supporting civilians and industry and delivering tangible action on cybersecurity issues that matter most to American communities and businesses.

2. **Workforce Development and Expertise:** The NSA and CISA's efforts in cybersecurity also contribute to developing a skilled workforce and advancing expertise in this field. These agencies collaborate with industry, government stakeholders, and academia to modernize cryptography and scale cybersecurity solutions.

3. **Technological Advancement in Cybersecurity:** The establishment of the AI Security Centre by the NSA and the focus on modernizing cryptography indicate the United States' commitment to using advanced technologies in cyber defence.

4. **Threat Intelligence and Information Sharing:** The NSA's collaboration with U.S. government partners, foreign partners, and the Defence Industrial Base enhances the nation's capability in threat intelligence and information sharing.

5. **Public Awareness and Education:** The strategy's focus on providing better support to civilians and industry underlines the importance of public awareness and education in cybersecurity.

While considering economic, geographic, demographic, and cultural similarity among the Five Eyes nations it became apparent that simply emulating one or more of the nations may not necessarily provide a good model for future improvements. Therefore, the author also considered how Singapore and Estonia are defending their critical national infrastructure. These were not included in the numerical analysis for the purpose of inclusion into the quadrant shown in Figure 1 above, but each were analysed with similar rigor regarding each attribute to capture details for this analysis. Following is a brief rationale for why these two nations may provide a good comparison as well as grounds for learning:

5.2.6 Singapore

Economy and Population:

Singapore is a small island city-state with a population of approximately 5.7 million people. It has a highly developed and diverse economy, driven by industries such as finance, trade, manufacturing, and technology. Like New Zealand, Singapore is considered a developed country with a relatively small population as compared to some of the larger economies.

Cyber Security Strategy:

Within the cyber security community, Singapore is known for its advanced approach to cyber security, especially in critical infrastructure and OT protection. The country has implemented a comprehensive and multi-faceted strategy to safeguard its digital assets and critical systems. Some notable aspects of Singapore's cyber security strategy include:

- Strong Regulatory Framework: Singapore has enacted laws such as the *Cybersecurity Act*, which provides a legal framework for the regulation and oversight of critical information infrastructure (CII) sectors. The Act mandates reporting of security incidents and enforces compliance with cyber security standards.
- Public-Private Collaboration: Singapore encourages collaboration between the government, private sector, and academia to collectively address cyber threats. The Cyber Security Agency of Singapore (CSA) plays a key role in coordinating efforts and providing guidance.
- National Cyber Security Masterplan: Singapore has developed a series of national cyber security masterplans that outline strategic objectives and initiatives to

strengthen cyber defence capabilities, including those related to OT and CNI protection.

- Education and Training: The country places emphasis on developing a skilled cyber security workforce. Initiatives like the Singapore Cybersecurity Consortium and collaborations with universities focus on research and training.
- International Engagement: Singapore actively participates in international forums and initiatives related to cyber security. This engagement helps the country stay updated on global threats and best practices.
- CII Designation: Singapore designates critical sectors such as energy, water, and healthcare as CII, subjecting them to higher security standards and regulatory requirements than less critical sectors.
- Incident Response: The country has a well-established incident response framework that ensures rapid and coordinated action in the event of cyber security incidents.

Following is an analysis of some of the relevant attributes for Singapore:

5.2.6.1 Cyber Defence of Critical Infrastructure

1. **Definition of CNI and Security Measures**: Singapore's Definition of CNI and Security Measures are robust, especially in sectors such as Aviation, Banking and Finance, Energy, Government, Healthcare, and Water. The country conducts nationwide cyber crisis management exercises, such as Exercise Cyber Star (XCS23), to improve crisis response capabilities and readiness against a wide range of cyber-attack scenarios on critical sectors using operational technology (OT) systems.[lxvii]
2. **Incident Response for CNI**: The Cyber Security Agency of Singapore (CSA) leads incident management and response, as evidenced in exercises like XCS23. These exercises focus on cross-sector incident management and emergency response plans for a range of cyber-attack scenarios, ensuring quick and effective national-level responses to cyber incidents. Singapore's government displays strong leadership and provides resources to support reporting and response activities through adequate resources.[lxviii]
3. **Investment in CNI Protection**: Singapore invests significantly in its cybersecurity sector. The Cybersecurity Talent, Innovation & Growth (Cyber TIG) Plan involves

an investment of S$50 million to uplift the cybersecurity sector, aiming to enhance the ecosystem and talent pipeline crucial for long-term protection against cyber threats.[lxix]

4. **Public-Private Partnerships in CNI Defence**: Public-private partnerships are a vital component of Singapore's cybersecurity strategy. The CSA's collaboration with Microsoft and Google are examples that illustrate their engagement in such partnerships, in which information, analysis, and intelligence on cyber threats are shared. These partnerships also include joint investigations and capacity-building initiatives.[lxx]
5. **Regulatory Compliance for CNI Security**: Singapore has strong enforcement of legislation and is revising its *Cybersecurity Act* to address the evolving cyber landscape. The *Cybersecurity (Amendment) Bill* focuses on updating existing laws for the protection of critical information infrastructure and extending coverage to other important systems and infrastructure.[lxxi]

5.2.6.2 Cybersecurity Preparedness

1. **National Cybersecurity Strategy**: Singapore's *Cybersecurity Strategy 2021* underlines its commitment to developing a vibrant cybersecurity ecosystem and a robust talent pipeline. This strategy aims to protect Singapore from cybersecurity threats and to strengthen its position as a trusted global business hub.
2. **Workforce Development and Expertise**: The Cyber TIG Plan supports innovation and steps up talent development efforts. It includes programs for mid-career conversions into cybersecurity and aims to professionalize the cybersecurity workforce. This effort contributes to meeting the demand for skilled cybersecurity professionals.
3. **Technological Advancement in Cybersecurity**: Singapore focuses on technological advancement in cybersecurity. This focus includes guidelines for CII owners to securely connect systems to 5G services and practices to combat sophisticated cyber-attacks. Additionally, Singapore is innovating in cyber security standards for blockchain enabled use cases through guidance provided through the published *Advisory on the Secure Development and Provisioning of Distributed Ledger Technology (DLT)-enabled Services* [lxxii] and by leading a discourse on *Guidelines for Secure AI System Development*[lxxiii].

4. **Threat Intelligence and Information Sharing**: Collaboration with Google and Microsoft exemplifies Singapore's commitment to threat intelligence and information sharing. This partnership helps build a comprehensive database of threats and vulnerabilities and supports joint investigations and operations.
5. **Public Awareness and Education**: Singapore is committed to raising public awareness and promoting education on cybersecurity. Initiatives like the SG Cyber Safe Partner Programme and Cyber Essentials mark certification illustrate the government’s efforts to encourage the adoption of good cybersecurity practices and to recognize organisations' efforts in this domain.

5.2.7 Estonia

Another country closely comparable to New Zealand in terms of its economy and population ratio but which has a more comprehensive cyber security strategy for defending CNIs and respective OT and ICS assets, is Estonia.

Following are some of the reasons why Estonia is a good fit for this comparison:

- Similar economy and population ratio: Estonia has a similar economy and population to New Zealand. In 2022, Estonia's GDP was $32.5 billion, and its population was 1.3 million. New Zealand's GDP was $210 billion, and its population was 5 million.
- Stronger cyber security strategy: Estonia has a stronger cyber security strategy than New Zealand. Estonia has a national cyber security strategy that takes a risk-based approach. The strategy includes a number of measures to protect OT and CNI, such as mandatory security requirements for critical infrastructure providers and a national cyber security centre.
- Estonia suffered significant cyber-attacks in the past and took learnings from responding to those to build a vision for its cyber defence with sustainability in mind.

Following is an analysis of some of Estonia’s attributes:

5.2.7.1 Cyber Defence of Critical Infrastructure

1. **Definition of CNI and Security Measures**: The Estonian Information System Authority (RIA) coordinates the development and administration of information systems to ensure interoperability and organizes activities related to information

security. It also handles security incidents in Estonian computer networks. The cyber defence of critical infrastructure includes maintaining the trouble-free functioning of the country's essential information and communication systems, with RIA playing a pivotal role in organizing protection on a national level for both public and private sector network and information systems essential for the functioning of the state.[lxxiv]

2. **Incident Response for CNI**: Estonia has implemented various initiatives to bolster defences against cyber-attacks. This includes the establishment of a ‘Red Team’ by CERT-EE to identify and address vulnerabilities before they are exploited by criminals. The Information System Authority has also introduced additional layers of protection to state systems and developed innovative tools to improve monitoring capabilities and swift response to cyber threats.
3. **Investment in CNI Protection**: Estonia's ongoing investment in cyber defence, including the adoption of new technologies and the development of cybersecurity infrastructure, highlights its commitment to protecting critical national infrastructure. The fact that it dedicated 30 million euros to cyber security in 2023[lxxv] with an additional 23 million euros allocated in 2024[lxxvi] displays its ongoing commitment to maintaining defence in the evolving threat landscape.
4. **Public-Private Partnerships in CNI Defence**: Estonia has built up its cyber defence partly by drawing upon the talents of the private sector, including a unit of volunteer cyber defences, the Cyber Defence League. This group consists of leading IT experts who donate their time to help the government face cyber threats.[lxxvii] Culturally this aligns well with the values and standards of how Aotearoa operates.
5. **Regulatory Compliance for CNI Security**: Estonia's cybersecurity standard, E-ITS, took effect in January and applies to a wide range of public and private sector entities. It compels organisations to map assets and risks, implement stronger safeguards, and adopt concrete preparation and response measures in the event of cyber-attacks.[lxxviii]

5.2.7.2 Cybersecurity Preparedness

1. **National Cybersecurity Strategy**: Estonia's National Security Concept, updated in response to the evolving international security environment, underlines its

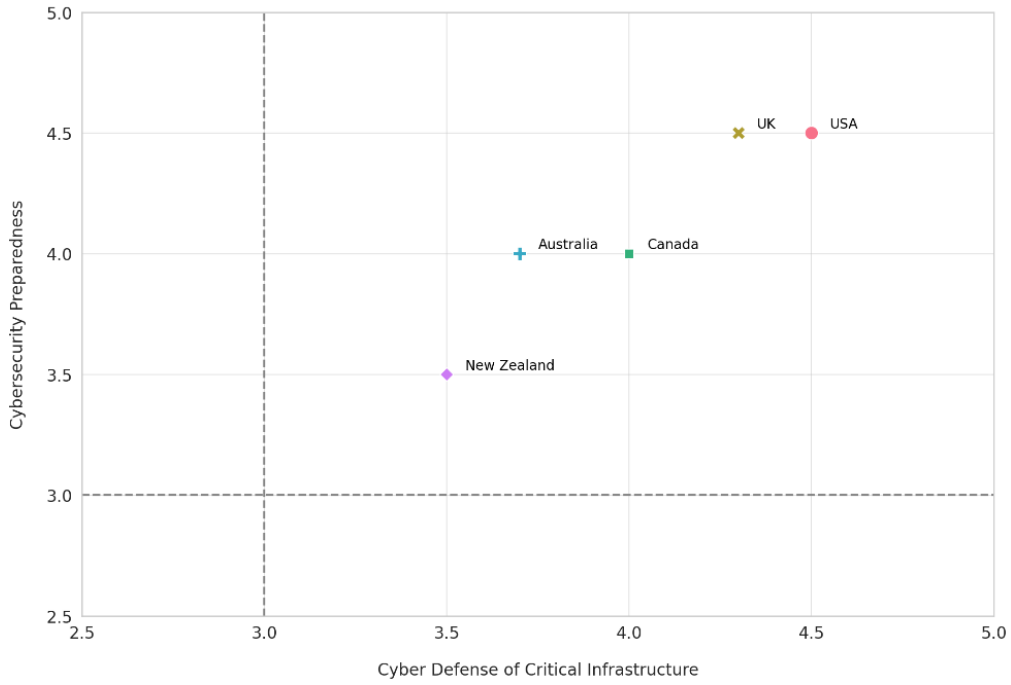
strategic approach to cybersecurity, with a focus on countering threats and enhancing national security.

2. **Workforce Development and Expertise**: Estonia's focus on cybersecurity workforce development is evident in initiatives such as the Cyber Battle events for youth, aimed at bringing new talent to the field and providing hands-on experience in cybersecurity.
3. **Technological Advancement in Cybersecurity**: Estonia leverages advanced cybersecurity technologies, as demonstrated by its collaboration with companies specializing in sophisticated cyber security training platforms and cyber ranges.
4. **Threat Intelligence and Information Sharing**: Estonia's participation in international exercises and collaborations, such as NATO's Cyber Coalition, illustrates its commitment to sharing and gaining insights on cyber threats and intelligence.
5. **Public Awareness and Education**: The country places a significant emphasis on raising public awareness about cybersecurity. This is evident in efforts such as cyber hygiene training, which is provided to polling station staff and political candidates and which highlights the importance of educating various sectors of society about cyber threats.

5.3 Summary of Literature Analysis for Five Eye Countries

Upon analysing the above attributes for each country in the Five Eyes alliance, the USA and the UK stand out as leaders, with Canada following closely and Australia and New Zealand emerging in their capabilities. The rating mechanism in line with the CCDM framework that led to the rankings in the following figure is further described in this section. The focus of the thesis was primarily on the five eyes countries; therefore, figure one compared only those nations. However, as Singapore and Estonia were also considered in the analysis, especially for some key attributes such as culture, population, GDP similarities and their commitment to cyber security – these two nations were also taken into consideration during the development of the conclusions and outcomes of this thesis.

Figure 1: Current state of cybersecurity preparedness for Five Eyes nations



Please Note

- The scores reflect a subjective analysis of each country's capabilities and initiatives in examined areas. The analysis and sources are noted below. **5 (Highest Rating):** Indicates excellence or a very high level of achievement in the specific attribute. **4 (High Rating):** Reflects a strong performance, albeit with some room for

improvement. **3 (Moderate Rating):** Suggests average performance, with notable areas for development.

- The sources of information on the relevant national organisations or initiatives related to cybersecurity in each country are noted in the detailed subjective analysis section below. They offer insights into the respective nation's approaches to cybersecurity preparedness and defence of critical infrastructure.
- This table is not exhaustive and as it is meant only to provide a subjective understanding for the purpose of how these countries compare in specific cybersecurity attributes to support the thesis.

The following table provides the detailed scores with a brief rationale for each of the Five Eyes countries from the analysis, and the table below explores further capabilities that make up the sum for these scores:

Table 4: Five Eyes Nations Scores and short rationale

Nation	Cyber Defence of CNI	Cybersecurity Preparedness	Rationale
USA	4.5	4.5	High investment in cybersecurity, advanced threat intelligence sharing and technology, and strong public-private partnerships.
UK	4.3	4.5	Robust cybersecurity strategies, active in international cooperation, and significant focus on enforcement of legislation and standards on CNI.
Canada	4.0	4.0	Effective policies and growing investment in cybersecurity, but still developing in comparison to USA and UK when it comes to alignment on the provincial level standardisation and coverage across all CNIs.
Australia	3.7	4.0	Strong legislative framework and practices emerging, but geographic isolation for various provinces within Australia poses unique challenges in standardizing implementation and in contributing to global cybersecurity cooperation.
New Zealand	3.5	3.5	Good public awareness programs and initiatives being planned and incident response improving, but limited resources, policies, and legislation as compared to larger counterparts.

The following table outlines further detailed scoring for each attribute along with a short rationale for each of the Five Eyes nations:

Detailed Scores Table

Table 5: Detailed Scores for attributes examined.

Attribute / Country	USA	UK	Canada	Australia	New Zealand
Cyber Defence of Critical Infrastructure					
Definition of CNI and Security Measures	4.6: Advanced definition of CNI; strong legislative framework	4.3: Well-defined CNI; significant investment, especially in finance and energy	4.1: Growing focus, slightly behind USA and UK	3.9: Solid measures with SOCI amendment; emerging, challenges in remote areas	3.7: Progressive measures, limited by resources and lack of CNI definition
Incident Response for CNI	4.7: Highly responsive, advanced capabilities such as CISA	4.5: Strong response capabilities backed by NCSC	4.0: Effective response but scaling up to match peers with CCCS	3.8: Developing capabilities; good agency coordination with ASD and ACSC	3.5: Capable but smaller scale operations and lack of resources
Investment in CNI Protection	4.8: Leading in investment, both public and private sectors	4.4: High investment, especially after recent incidents	4.2: Increasing investment in energy and telecom	3.7: Steady investment and strong commitment after recent incidents	3.6: Investing, but on a smaller scale and no clear definition of CNI
Public-Private Partnerships in CNI Defence	4.5: Strong partnerships across CNI sectors	4.2: Active engagement of private sector in protection	4.1: Solid efforts, developing stronger partnerships	3.8: Building stronger public-private partnerships; recent changes to strengthen	3.7: Efforts are ongoing to develop a sustainable model
Regulatory Compliance for CNI Security	4.6: Strict regulations with enforcement in CNI sectors	4.3: Robust regulations, especially post GDPR	4.0: Developing stronger regulations and compliance	3.9: Aligned with international standards and enforcing with SOCI Act update	3.8: No common framework or enforcement; challenges in enforcement.
Cybersecurity Preparedness					
National Cybersecurity Strategy	4.7: Comprehensive and	4.6: Comprehensive strategy	4.2: Developing a	4.0: National strategy with	3.9: Developing strategy; focus

Attribute / Country	USA	UK	Canada	Australia	New Zealand
	effective national strategy	with international focus	comprehensive national strategy	regional considerations	on digital sectors and defining CNIs
Workforce Development and Expertise	4.8: High level of skilled workforce in cybersecurity	4.4: Growing cybersecurity workforce and expertise	4.1: Focused on building cybersecurity workforce	3.9: Growing focus on cybersecurity skills	3.7: Building workforce; emphasis on education
Technological Advancement in Cybersecurity	4.9: Leading in technological advancements	4.5: Focus on adopting new cybersecurity technologies	4.3: Investing in cybersecurity technology	4.1: Adopting new technologies; focus on innovation	3.8: Focus on leveraging technology for defence
Threat Intelligence and Information Sharing	4.8: Robust threat intelligence and information sharing	4.7: Effective threat intelligence and sharing mechanisms	4.4: Good threat intelligence and sharing practices	4.0: Effective information sharing, room for improvement	3.9: Good collaboration with Five Eyes, but smaller scale and gaps in sharing and gathering intelligence domestically
Public Awareness and Education	4.6: Strong public awareness and educational initiatives	4.5: Significant efforts in public education on cybersecurity	4.2: Increasing public awareness campaigns	4.1: Active in public education and awareness	3.8: Strong efforts in public awareness

6 Field Survey and Analysis

The survey was meticulously crafted to gather insights on the experts' view of, compliance with, and challenges faced in implementing good practices and frameworks within CNIs in New Zealand. It was also designed to probe the impact of the absence of standardised cybersecurity measures in New Zealand for CNIs, along with soliciting open opinions of experts on the current state and future strategy to gather information for subjective analysis. Questions were intentionally broad and open so as to provide sufficient coverage for the attributes and framework used for subjective analysis during the literature review so the results of the field survey could be synthesised to develop hypotheses. The following table lists questions that were presented to each of the experts and the respective objectives:

Table 6: Survey Questions and Objectives

Question	**Objective**
1. What are the key challenges and vulnerabilities facing OT systems within CNIs in New Zealand?	To identify specific challenges and vulnerabilities in New Zealand's OT systems, utilizing industry expert insights for developing effective security measures.
2. Are there any existing OT security frameworks, standards, or regulations in New Zealand? How effective do you think they are?	To assess the current regulatory landscape's effectiveness, with industry experts providing perspectives on existing frameworks, standards, and potential improvements.
3. What are some best practices you have observed in other countries or industries for securing OT environments?	To learn from global best practices in OT security, with experts sharing insights that can inform hypotheses for New Zealand.
4. In your opinion, what role should the New Zealand government play in supporting OT security within CNIs? What initiatives or policies would you suggest?	To determine the government's role in OT security within CNIs, gathering expert suggestions on potential initiatives or policies.
5. How can collaboration between the government, industry, and academia enhance OT security efforts within CNIs?	To explore ways to enhance OT security through collaboration between government, industry, and academia, based on expert perspectives.
6. Do you see any gaps in communication or information sharing among various	To identify communication or information sharing gaps among OT security

Question	**Objective**
stakeholders in the OT security community within the CNIs?	stakeholders, aiding in hypothesis development for improvements.
7. What impact could mandatory reporting of OT security incidents have on improving overall security?	To evaluate the potential impacts of mandatory OT security incident reporting on overall security, based on industry expert insights.
8. Are there any emerging technologies or trends that could significantly affect OT security?	To pinpoint emerging technologies or trends affecting OT security in CNIs, gathering expert opinions on their potential impact.
9. What incentives or benefits do you think would encourage organisations to invest more in OT security within CNIs?	To identify incentives or benefits that could motivate organisations to invest in OT security within CNIs, as seen through the lens of industry experts.
10. What are your thoughts on capacity building and skill development for OT security professionals in New Zealand?	To assess the need for capacity building and skill development among OT security professionals in New Zealand, drawing from expert insights on required skills and training.
11. In your opinion, what should be the long-term goals for enhancing OT security in New Zealand?	To establish long-term goals and strategic initiatives for enhancing OT security, based on expert perspectives.
12. Do you have any recommendations or key takeaways for policymakers and industry leaders to strengthen OT security in New Zealand? Or, if you were a policymaker or an industry leader within CNI or government for a day, what would you prioritise to strengthen cyber security in New Zealand?	To gather open-ended recommendations and key takeaways from industry experts, aimed at informing policy and practice development to strengthen cybersecurity in CNI.

The survey was distributed through multiple channels, including online platforms and direct mail, to ensure a comprehensive reach and robust response rate. Over thirty (30) experts who had experience in defending or operating with CNIs and exposure to securing OT and ICS environments within New Zealand were contacted. A dozen of these experts

were surveyed through video calls between the experts and the researcher directly so as to foster candid conversation and open data collection. The list of industries from which the experts were surveyed includes:

- Government Services
- Energy Generation, Distribution and Retail
- Supply Chain and Logistics
- Professional Cyber Security Services for CNIs
- Gas Refinery and Distribution
- Dairy and Food Manufacturing
- Operational Technology Service Providers
- Manufacturing
- Telecommunications
- Water

This array of sectors indicates a comprehensive representation across both critical infrastructure and essential services within New Zealand. The surveyed group of experts, encompassing a diverse range of seniority and expertise levels, is characterised by key attributes detailed below:

- Executives: Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs)
- ICS and OT SMEs: OT operators, engineers and cyber security experts
- Cybersecurity service providers for multiple CNIs and government agencies
- Representatives from various age groups and ethnicity
- Professionals skilled in risk management and governance expertise

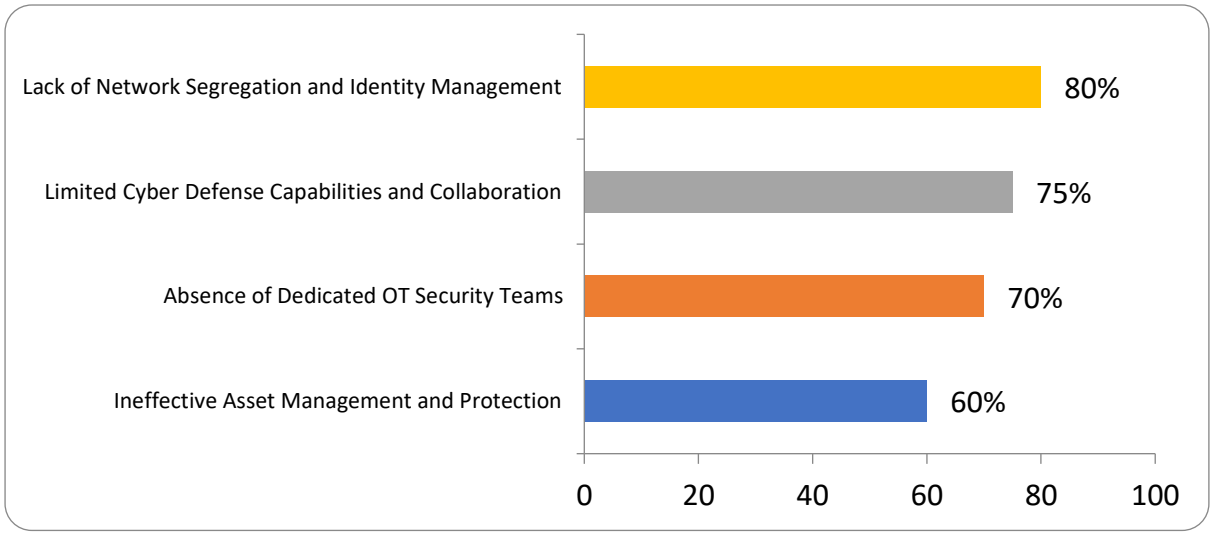
Unfortunately, no female representatives accepted the invitation for the survey and given a small talent pool and even a smaller pool of experts with OT and ICS experience this represents an already acknowledged issue of gender gap within the cyber security workforce. The characteristics outlined above collectively underscore a group with a comprehensive blend of leadership, technical proficiency, industry-specific knowledge, and cross-generational insights - all crucial for a nuanced understanding of cybersecurity within the context of CNIs, to obtain comprehensive input.

6.1 Analysis of Input from the Industry Experts

This thesis now delves into the insights and perspectives offered by the distinguished professionals who are at the forefront of cybersecurity within the CNI in New Zealand and who have defended OT and ICS environments. This diverse group encompassed expertise spanning multiple CNIs—including essential government services—and over a dozen distinct industries. These experts bring a wealth of practical experience in operational, governance, and risk management domains. The analysis further benefits from the inclusion of diverse age groups, adding a dynamic range of generational insights. Together, their collective input forms the following highlights for our review, providing a view of the challenges and strategies pivotal to safeguarding New Zealand's CNI. Some key insights are summarised in graphs with major themes as follows, with further detailed analysis below:

6.1.1 Key Challenges and Vulnerabilities

Figure 2: Key Challenges and Vulnerabilities



Lack of Network Segregation and Identity Management (80% of experts)

- Experts consistently noted a systemic issue with network infrastructure, particularly the absence of proper network segregation, which is critical for safeguarding OT systems against cyber threats.
- The inadequate implementation of identity and access management protocols was a recurrent concern, pointing to vulnerabilities in controlling and monitoring system access.

Limited Cyber Defence Capabilities and Collaboration (75% of experts)

- A majority pointed out the insufficiency in both cyber defence skills and a collaborative approach within organisations. This includes a reluctance to share knowledge and resources across different departments, hindering effective cybersecurity strategies.
- The lack of skilled personnel in cyber defence is a critical issue, undermining the ability of organisations to adequately defend against and respond to cyber threats.

Absence of Dedicated OT Security Teams (70% of experts)

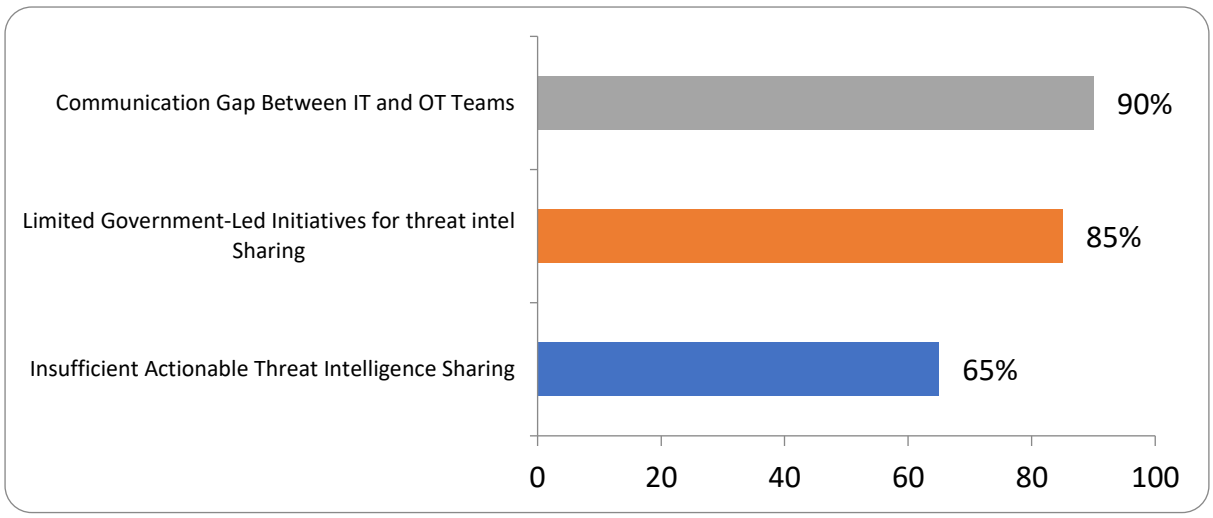
- A significant number of experts highlighted the lack of specialised OT security teams. This gap often results in OT security responsibilities being inadequately managed by IT personnel, who may not have specific expertise in OT systems.
- This lack of specialisation can lead to a misunderstanding of the unique requirements and risks associated with OT environments.

Ineffective Asset Management and Protection (60% of experts)

- Many experts emphasised the failure to properly manage and protect critical assets within OT systems. This includes a lack of focus on identifying and securing 'crown jewels'—the most critical components of the infrastructure.
- This oversight can lead to vulnerabilities in the system, as the most crucial assets may not receive the necessary level of protection.

6.1.2 Communication and Information Sharing Issues

Figure 3: Communication and Information Sharing Gaps



Communication Gap Between IT and OT Teams (90% of experts)

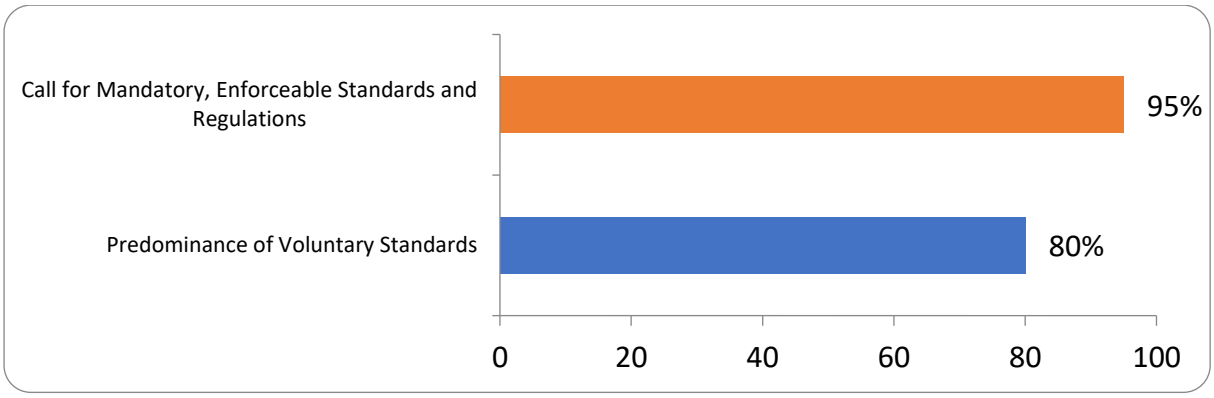
- Nearly all experts observed a significant communication gap between IT and OT teams, leading to a lack of mutual understanding and collaboration. This disconnect hinders the development of cohesive and comprehensive security strategies.
- The absence of a unified approach can result in security measures that are either inefficient or inadequate for the specific needs of OT systems.

Insufficient Actionable Threat Intelligence Sharing (65% of experts)

- A significant portion of experts stressed the inadequacy in sharing actionable threat intelligence, which is crucial for pre-emptive defence strategies against emerging cyber threats.
- The lack of effective intelligence sharing mechanisms, both within organisations and at a national level or government led initiatives, limits the ability to respond proactively to cybersecurity challenges.

6.1.3 Lack of Frameworks and Regulations:

Figure 4: Themes related to OT Security Frameworks, Standards, and Regulations



Call for Mandatory, Enforceable Standards and Regulations (95% of experts)

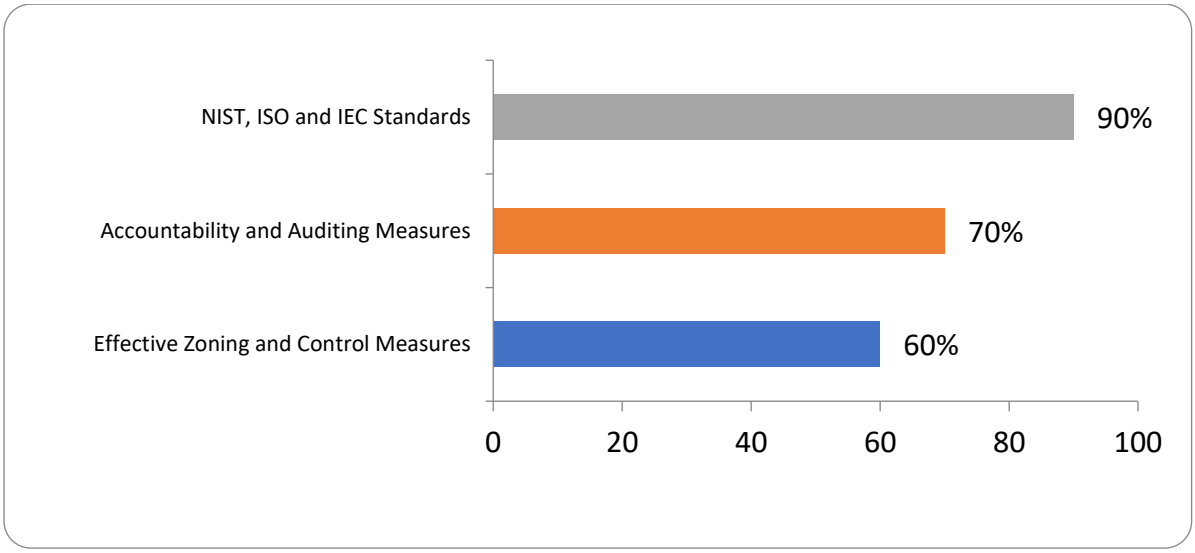
- Almost unanimously, experts advocated for the implementation of mandatory and enforceable standards and regulations. This is seen as critical to establishing a baseline of security practices that all organisations must adhere to.
- Such regulations would also provide a framework for accountability and continuous improvement in OT security practices.

Predominance of Voluntary Standards (80% of experts)

- Many experts pointed out the reliance on voluntary standards such as NIST, IEC and ISO, which, while valuable, lack the enforceability needed to ensure widespread compliance.
- The voluntary nature of these standards often leads to inconsistent application and a varied level of security posture among organisations.

6.1.4 Lack of Enforcement and Common Standards

Figure 5: Lack of enforcement and common standards



NIST ISO and IEC Standards Used Where feasible. (90% of experts)

- Many experts pointed out that the reliance on voluntary standards such as NIST, IEC and ISO, which, while valuable, lacks the enforceability needed to ensure widespread compliance.

Accountability and Auditing Measures. (70% of experts)

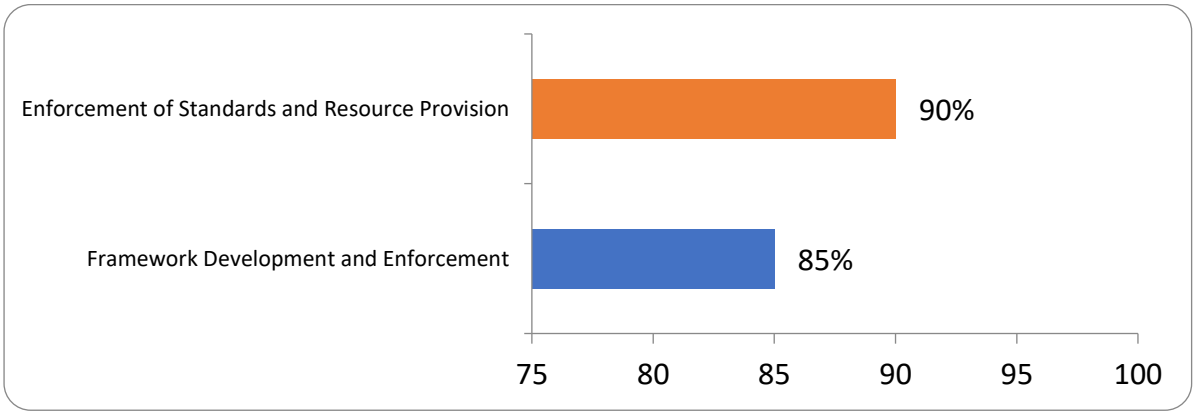
- Many experts believed that most leadership within CNIs don't feel personally responsible or accountable for cyber defence measures as there is no enforcement and no personal ramifications for them or their organisations if good standards are not followed.
- Experts suggested imposing financial penalties or prosecution for directors of non-compliant organisations, creating personal accountability for leaders, and offering funding, education, or support to organisations that demonstrate better cybersecurity practices.

Effective Zoning and Control Measures (60% of experts)

- Many experts highlighted that effective zoning and control measures are seen as crucial in safeguarding CNIs and OT. The success of these measures is often attributed to the implementation of robust frameworks, proper segregation and zoning, and a culture of accountability and auditing.

6.1.5 Role of the NZ Government in developing and enforcing standards

Figure 6: Role of the New Zealand Government



Enforcement of standards and resource provision (90% of experts)

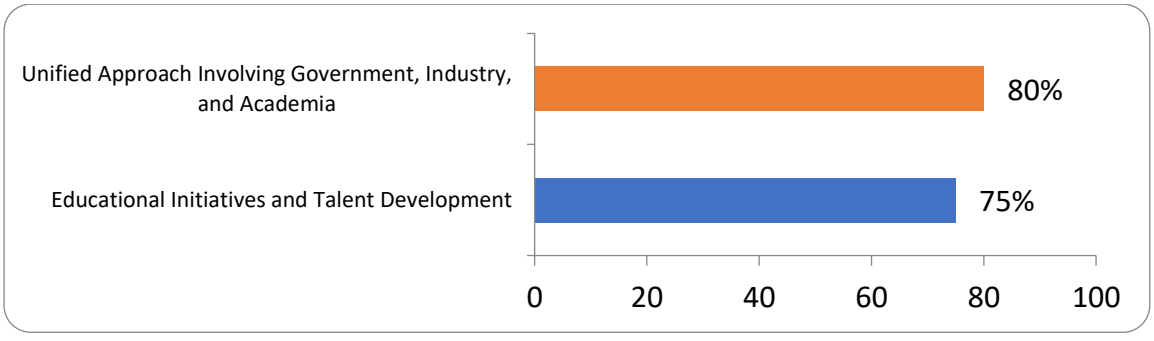
- Experts expressed concern that New Zealand is not ready for long-term goals in this area, citing the impracticality of the current New Zealand Information Security Manual (NZISM) and a lack of budget and resources.

Framework development and enforcement (85% of experts)

- Experts suggested that there needs to be a mandatory standard for IT and OT security in New Zealand, similar to standards such as the SOCI Act in Australia or the European model. The current voluntary standards, including the NCSC Cyber Security Framework (CSF), are not seen as sufficient.

6.1.6 Lack of Collaboration and Awareness

Figure 7: Focus areas in Collaboration Enhancement



Unified Approach Involving Government, Industry, and Academia (80% of experts)

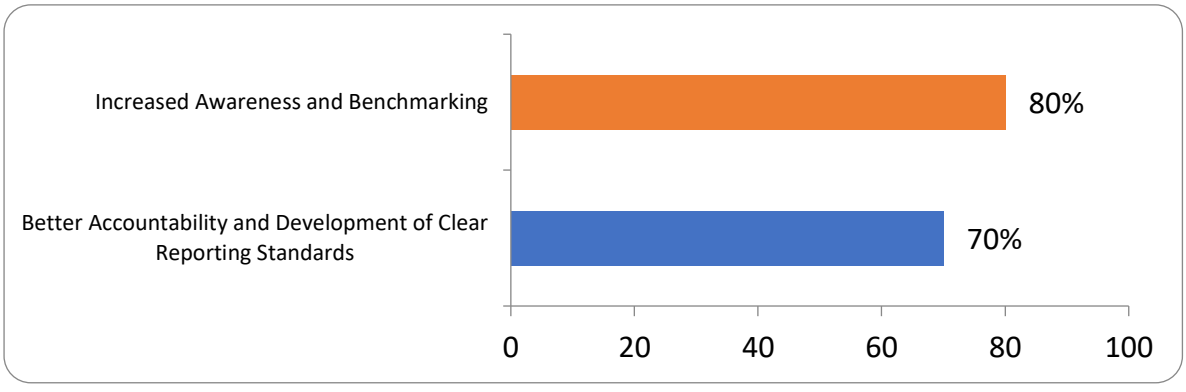
- Experts emphasised the threefold benefits of collaboration - improved awareness, the implementation of frameworks, and enhanced tactical threat intelligence sharing. There is a suggestion that the New Zealand government needs to work closely with industry and academia to prevent brain drain and encourage knowledge sharing.
- A need for government-level expertise in operational technology (OT) security is highlighted, with security leadership reporting directly to the boards of organisations. There is also a call for the government to be more involved in a meaningful way, by taking such action as setting up baseline standards and improving information sharing across sectors.

Educational Initiatives and Talent Development (75% of experts)

- Starting with education was seen as crucial. Affordable and accessible resources for education, along with the enforcement of laws and policies, are recommended. The government is encouraged to improve the cybersecurity talent pool in New Zealand and gain worldwide recognition for its cybersecurity education.
- Concerns were raised by experts about New Zealand not being ready for long-term goals due to impractical standards like NZISM, and a lack of budget and resources. More collaboration between government and other sectors, a change in people's attitudes, and providing better remuneration for cyber talent in New Zealand are suggested as ways to improve the situation.

6.1.7 Impact of Mandatory Reporting

Figure 8: Impact of Mandatory Reporting of cyber security incidents



Increased Awareness and Benchmarking (80% of experts)

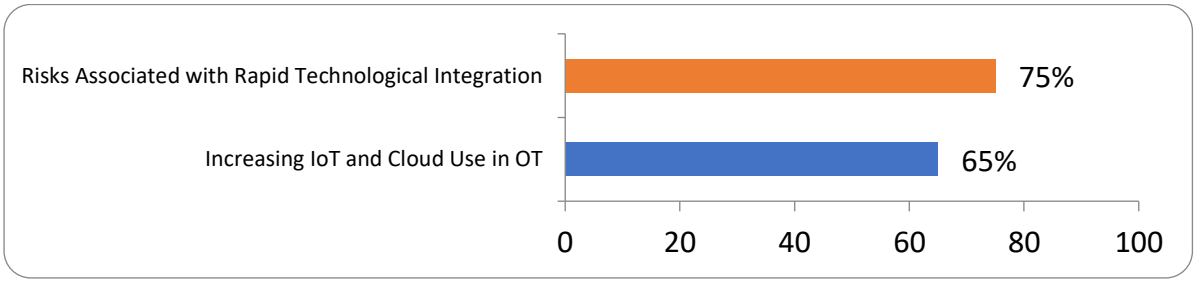
- There is a need for more awareness and education in cybersecurity, particularly in combining IT and OT education. However, the current lack of government requirements and funding for training is seen as a barrier to increasing awareness effectively.
- The government is urged to take an active role in building awareness about cyber threats, especially in the context of OT security. This includes educating industry leaders and government officials who may not fully understand the nuances of OT security.
- Experts suggest making CNI security a priority and consistently educating the population about it. They advocate for the use of frameworks and the need for consistent funding to ensure that cybersecurity initiatives are sustained across different government administrations.

Better Accountability and Development of Clear Reporting Standards (70% of experts)

- There is a consensus on the need for mandatory reporting for cybersecurity incidents. However, experts emphasise the importance of not just making this mandatory but also providing guidance on how, what, and when to report. They pointed out that currently no accountability and that the government doe not provide a guiding hand for CNIs on these matters. Mandatory reporting, if confidential, is seen as a way to improve awareness and uplift cybersecurity practices.
- By implementing these reporting standards, risk assessments will become easier, providing tangible and quantifiable data that can help others learn. It is important to educate organisations on the difference between OT and IT security and the specifics of what and when to report.

6.1.8 Emerging Technologies and Trends to Watch

Figure 9: Emerging Technologies and Trends to Watch



Risks Associated with Rapid Technological Integration (75% of experts)

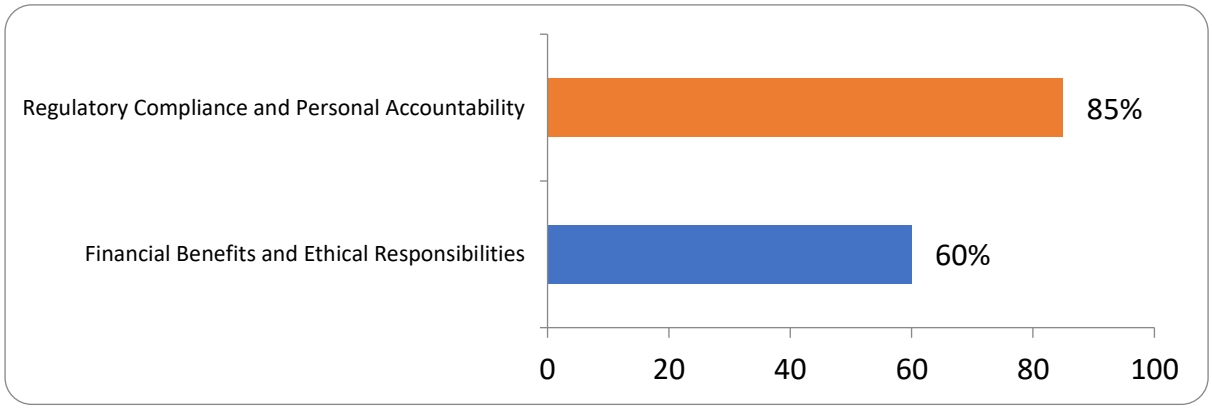
- The interconnection of systems has made OT systems more vulnerable than in the past. The lack of sufficient cybersecurity knowledge among control engineers and a shortage of SMEs in New Zealand are contributing to this vulnerability.
- There is a noted challenge in the relationship between IT and OT personnel. The lack of understanding and trust between these groups, combined with the separation of OT from IT and other technologies, creates potential for conflict and miscommunication.

Increasing IoT and Cloud Use in OT (65% of experts)

- The integration of IoT and cloud technologies into OT environments is seen as risky and dangerous. Data sharing from OT to business introduces new connections into the OT environment, eroding the concept of air-gapping and introducing new risks. Service providers and engineers are also contributing to these risks, even though visibility is improving through better monitoring.
- Despite the risks, the introduction of advanced technologies into OT environments is also seen as having a positive impact. It increases awareness about security and the role of defence in depth. Some experts noted that OT devices are becoming more intelligent and capable of better monitoring and encryption, thanks to these new technologies.

6.1.9 Possible incentives to invest in OT security in CNI.

Figure 10: Incentives for OT Security Investment in CNIs



Regulatory Compliance and Personal Accountability (85% of experts)

- The implementation of frameworks and enforcement by the government is seen as crucial to change behaviour. There is a call for financial penalties or prosecution for directors of non-compliant organisations. Experts suggest that compliant

organisations should be rewarded, while non-compliant ones should face punishment. Personal accountability for leaders is lacking, but if enforced by the government, such a measure could lead to a greater focus on securing operational technology (OT) assets.

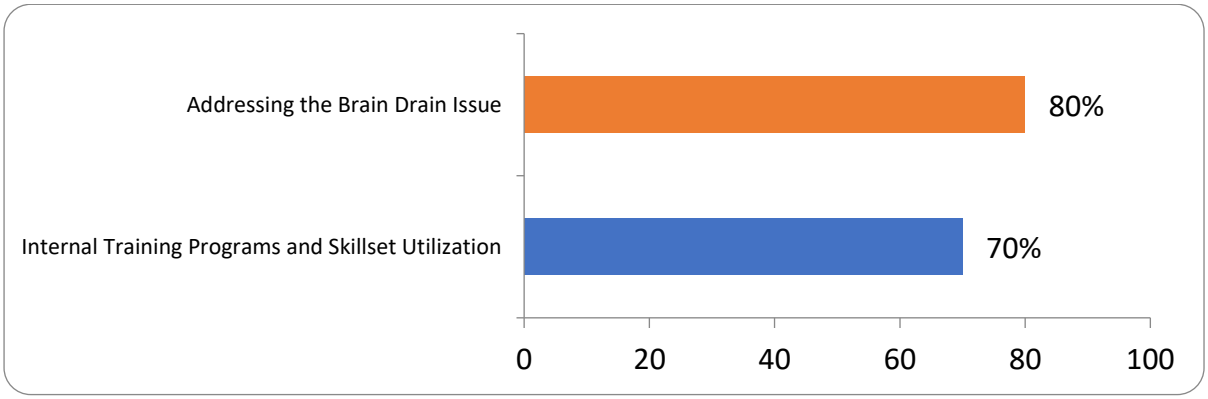
- Regulators need to enforce standards before considering incentives like tax rebates. Organisations must understand the value of cybersecurity, and government or national level mandates could provide incentives for leadership to prioritize cybersecurity. However, there is scepticism about the availability of significant incentives, especially in a challenging economic climate.

Financial Benefits and Ethical Responsibilities (60% of experts)

- Experts believe that while there may not be direct financial incentives for cybersecurity, organisations that meet baseline standards or regulatory requirements should be recognised. Cybersecurity needs to be treated with the same importance as health and safety, incorporating ethical and social responsibility. The potential financial benefits of improved cybersecurity could include reductions in insurance premiums, as seen in some Australian companies.

6.1.10 Lack of Workforce Development and Capacity Building Efforts

Figure 11: Key Improvements in Workforce Development and Capacity Building



Addressing the Brain Drain Issue (80% of experts)

- There is a significant concern about the brain drain in New Zealand, where skilled individuals are leaving due to inadequate salaries and limited exposure in the

cybersecurity field. Experts note the need for incentives to retain talent within the country.

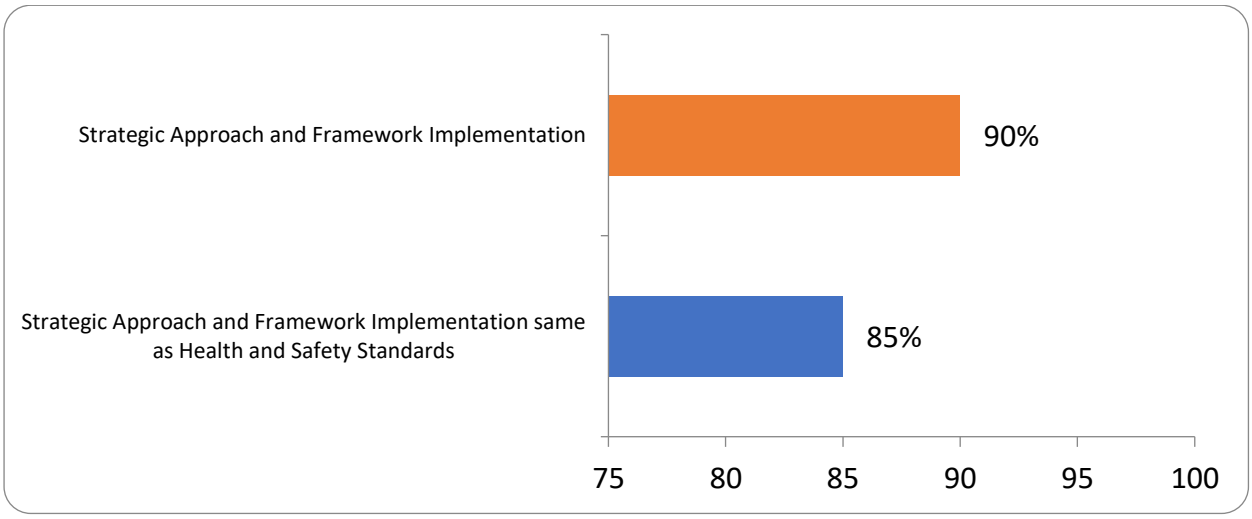
- Addressing the brain drain issue is seen as requiring a joint effort between the government and industry. This includes mentoring initiatives to bring more people, especially OT engineers, into cybersecurity. Reducing the cost of learning and providing better incentives for studying and working in cybersecurity in New Zealand are suggested as ways to mitigate the brain drain.

Internal Training Programs and Skillset Utilisation (70% of experts)

- Need for Government-Led Training Initiatives: Experts suggest that the government should organize efforts to scale the talent pool for cybersecurity, particularly within critical national infrastructures (CNIs). There is a call for more affordable and accessible training programs, as current options like SANS Institute courses are considered too expensive. The government should consider training people within CNIs, especially as not all organisations in New Zealand have the funding for this.
- Combination of IT and OT Education: The importance of combining IT and OT education is highlighted, with a focus on bringing people up to speed in cybersecurity skills and knowledge. However, there is a noted lack of funding for such training initiatives.

6.1.11 Consider Long Term Goals for Improving OT Security in CNI

Figure 12: Long Term Goals for Improving OT Security in CNI



Strategic Approach and Framework Implementation (90% of experts)

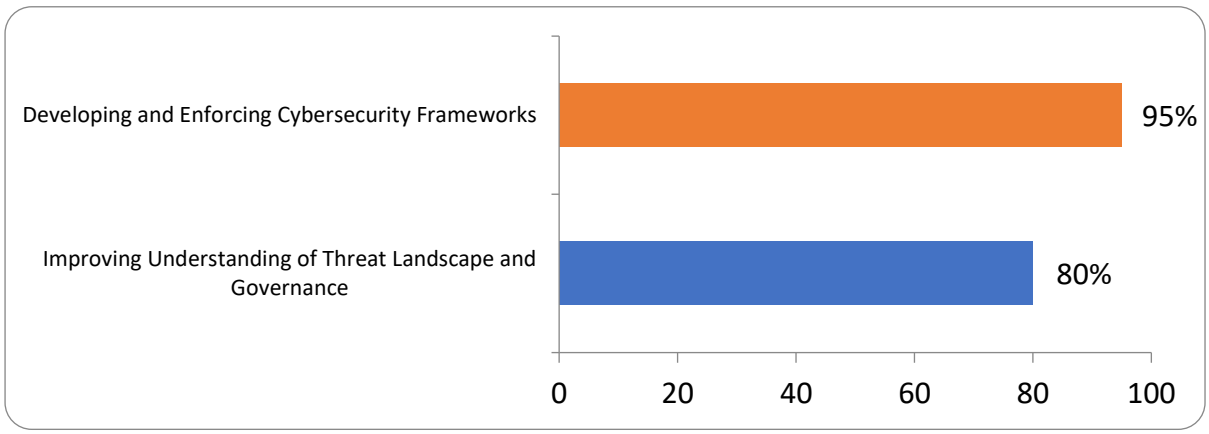
- The experts highlight the necessity of a strategic approach to cybersecurity, including the development and enforcement of frameworks and standards. This approach should encompass awareness, education, and the baseline application of standards across all CNIs. The implementation of such frameworks is seen as crucial for improving the overall cybersecurity posture of organisations and the country.
- There is an emphasis on the need for the government to regulate and hold directors and CEOs accountable for cybersecurity in their organisations. The experts believe that personal accountability, coupled with the government's enforcement of standards and policies, is key to a more effective cybersecurity strategy.

Strategic Approach and Framework Implementation same as Health and Safety Standards (85% of experts)

- Experts emphasise the need to make critical national infrastructure (CNI) security a priority, with consistent frameworks and education. They suggest using the example of WorkSafe, which built relationships with the industry during the COVID pandemic, as a model for cybersecurity. The long-term goal is to be less reactive and more proactive in securing the country's CNI, with a need for change in governance at the government level.
- Cybersecurity is seen as currently lagging behind health and safety in terms of standards and enforcement. The experts suggest that the New Zealand government should establish a separate entity to oversee and prescribe standards for CNI organisations and implement baseline auditing. This approach would not only check compliance but also raise awareness and educate organisations about cybersecurity. They propose looking at Singapore's model of holding boards accountable as a potential step forward.

6.1.12 Recommendations for Policymakers and Industry Leaders

Figure 13: Recommendations for Policymakers and Industry Leaders



Developing and Enforcing Cybersecurity Frameworks (95% of experts)

- The development and enforcement of frameworks and policies applicable to CNIs are seen as essential. Experts point out the current lack of proactive advice or education provided to CNIs and stress the need for clear guidelines for the protection of OT and ICS assets. They advocate for defining a standard for CNIs, developing methods for organisations to assess their maturity over time, and providing more education and awareness.
- There is a suggestion to use the WorkSafe innovation team as an example to build relationships with the industry. The long-term goal is to make CNI security a priority with consistent funding and support across different government administrations. Experts also highlight the need for awareness, education, and the application of baseline frameworks and standards.

Improving Understanding of Threat Landscape and Governance (80% of experts)

- Experts emphasise the need for a deeper understanding of the critical national infrastructure (CNI), its capabilities, and exposure to threats. They suggest that there should be a mandate covering the baseline application of standards and mandatory reporting for cybersecurity incidents. This approach includes providing actionable guidance and rolling out standards across all CNIs gradually. The focus is on building capacity, increasing awareness, and giving organisations a clear reason to improve their cybersecurity posture.
- There is a call for the government to be more involved in a meaningful way, including setting up baseline standards and improving information sharing. Experts

suggest that industry experts should frequently present and share the threat landscape to enhance collective understanding.

The charts and expanded notes above represent the most common and key responses from all surveyed experts. Additionally, some of the experts raised the following unique points to consider in enhancing New Zealand's capability to defend critical infrastructure:

Unique Challenges in New Zealand's Context:

- **Geographical Isolation:** New Zealand's remote location might create specific challenges in cybersecurity, such as delays in accessing international resources or expertise. Experts emphasised developing local capabilities and self-reliance in cybersecurity responses.
- **Small Market Dynamics**: The size and interconnectedness of New Zealand's market may necessitate customised cybersecurity strategies. Experts could have pointed out the need for solutions that are scalable and adaptable to smaller organisations, which are prevalent in New Zealand's economy.
- **Māori Involvement:** The inclusion of Māori perspectives in cybersecurity strategy could be a unique aspect. This approach might involve integrating Māori values and concepts into cybersecurity policies and practices, promoting diversity and inclusivity in security planning.
- **AI and Machine Learning**: Experts advocated for leveraging advanced technologies like AI and machine learning to predict and identify threats more efficiently, suggesting that these technologies could be pivotal in proactive defence mechanisms.
- **Blockchain for Security**: The suggestion to use blockchain technology could focus on enhancing data integrity and traceability in OT systems, especially in areas like supply chain security and identity management.
- **Cybersecurity as a Public Good**: Some experts proposed viewing cybersecurity as a public good, advocating for government-funded initiatives to ensure a baseline level of cybersecurity across all CNI organisations, especially benefiting smaller entities with limited resources.
- **Emphasis on Resilience:** Moving beyond prevention, the emphasis on building systems that are not just secure but also resilient to attacks could be a key insight.

This includes strategies for quick recovery and maintaining operational continuity in the face of cyber incidents.

- **Learning from Global Best Practices**: Unique suggestions might involve adopting a more structured approach to learning from global cybersecurity incidents and best practices. This includes not just adopting these practices but also adapting them to fit New Zealand's unique cybersecurity landscape.

Where relevant, these perspectives have been considered in the development of hypotheses in the following section.

6.2 CCDM Observations

Furthermore, for the purposes of aligning the field survey results with the literature analysis and structuring findings in the same categories as each of the countries analysed above, the following insights, along with challenges and recommendations shared by the experts, become apparent:

Cyber Defence of Critical Infrastructure

1. **Definition of CNI and Security Measures**
    - **Challenges:** Experts highlighted the lack of robust cybersecurity measures specific to CNI, including poor network segregation and identity management, and inadequate asset management.
    - **Recommendations:** Emphasise developing dedicated OT security teams, take measures to increase awareness, enhance education, and implement defendable architectures focused on the protection of critical assets.
2. **Incident Response for CNI**
    - **Challenges:** There is a noted deficiency in effective incident response strategies, partly due to the communication gap between IT and OT teams and the lack of collaborative approaches within organisations.
    - **Recommendations:** Enhance incident response capabilities by fostering better communication and collaboration between IT and OT teams and developing specialised incident response frameworks and exercises for CNIs.
3. **Investment in CNI Protection**
    - **Challenges:** Experts consistently raised concerns about inadequate governance, financial, and resource allocation towards CNI protection.
    - **Recommendations:** Increase investment in both technological solutions and human resources dedicated to OT security, focusing on areas such as asset protection and cyber defence capabilities.
4. **Public-Private Partnerships in CNI Defence**
    - **Challenges:** Current collaborations between government agencies and private sector entities are seen as insufficient, with a lack of effective mechanisms for information sharing and joint cybersecurity initiatives.

- **Recommendations:** Strengthen public-private partnerships through formal frameworks that facilitate information sharing, joint threat assessments, and cooperative defence strategies.

5. **Regulatory Compliance for CNI Security**

    - **Challenges:** A major concern is the reliance on voluntary standards with a call for mandatory, enforceable regulations.
    - **Recommendations:** Implement stringent laws and regulations governing CNI cybersecurity and establish mechanisms for their enforcement and compliance monitoring.

Cybersecurity Preparedness

1. **National Cybersecurity Strategy**

    - **Challenges:** There is an apparent lack of a comprehensive and effective national strategy dedicated to cybersecurity, particularly in addressing the unique challenges of OT security.
    - **Recommendations:** Develop and implement a national cybersecurity strategy that includes specific components for CNI protection and OT security.

2. **Workforce Development and Expertise**

    - **Challenges:** A significant skills gap and a shortage of cybersecurity professionals, exacerbated by the brain drain, were identified as major issues.
    - **Recommendations:** Invest in workforce development programs, including training and skill development initiatives, to build a robust pool of cybersecurity experts.

3. **Technological Advancement in Cybersecurity**

    - **Challenges:** There is a need for more advanced and effective cybersecurity technologies, especially in the context of emerging threats and the integration of new technologies in OT.

- **Recommendations:** Encourage the adoption and development of cutting-edge cybersecurity technologies, focusing on areas such as AI, machine learning, and secure cloud technologies for OT environments.

4. **Threat Intelligence and Information Sharing**

    - **Challenges:** The survey revealed a deficiency in the capability to gather, analyse, and share cyber threat intelligence effectively.
    - **Recommendations:** Establish and strengthen mechanisms for threat intelligence gathering and sharing, both within the government and across public-private sectors.

5. **Public Awareness and Education**

    - **Challenges:** There is a lack of public awareness and education about cybersecurity, which is crucial for national preparedness.
    - **Recommendations:** Implement national campaigns and educational programs to raise public awareness about cybersecurity risks and best practices.

The quantitative and qualitative analysis of survey responses surfaced and confirmed many insights gained through literature review when comparing to good practices employed by the leading countries within Five Eye Countries, Singapore and Estonia.

7 Hypotheses

Collectively, the reviews of the literature, landscape and expert input provided ample information to enable the development of the various hypotheses noted in this section. The thesis focuses on applicability and context in relation to New Zealand and therefore, in addition to examining Five Eyes countries, Singapore and Estonia were also considered as these two countries include characteristics in common with New Zealand and in the light of the good practices they employ in their protection of CNI and cyber defence preparedness. Based on the framework utilised to assess the effectiveness of each of the above countries and the attributes examined for each country, along with the input from the surveys and a study of the general best practices within the cyber security community, this thesis highlights the following ten (10) priority areas for New Zealand to consider in its efforts to improve the cyber security of the CNIs. Many of these elements may apply to all CNIs, regardless of the absence of OT and ICS environments.

7.1 List of areas for the development of hypotheses based on CCDM.

To improve the cybersecurity of CNIs operating OT and ICS environments in New Zealand, the following measures are essential:

1. **Strengthen Definition of CNI and Security Measures:**
    - Define CNIs and ensure proper asset management, prioritizing the protection of critical assets.
    - Develop or adopt and implement dedicated OT security frameworks and standards.
    - Focus on robust network segregation and identity management.
2. **Enhance Incident Response for CNI:**
    - Establish specialised incident response teams for OT and ICS environments.
    - Foster effective communication and collaboration between IT and OT teams.
    - Create and regularly update incident response plans specific to CNI.
3. **Increase Investment in CNI Protection:**
    - Allocate more financial resources and expertise towards securing OT and ICS.

- Invest in advanced cybersecurity technologies tailored for OT environments.
- Support research and development in OT-specific cybersecurity solutions.

4. **Foster Public-Private Partnerships in CNI Defence:**
    - Build formal frameworks for collaboration between government and private sector entities.
    - Encourage information sharing and cooperative defence strategies.
    - Promote joint initiatives for threat intelligence and incident response and allocate dedicated funding and resources to sustain them.
5. **Ensure Regulatory Compliance for CNI Security:**
    - Move from voluntary to mandatory and enforceable cybersecurity standards.
    - Implement stringent regulations specific to OT and ICS within CNIs.
    - Establish a regulatory body to monitor compliance and enforce standards for CNIs.
6. **Develop a Comprehensive National Cybersecurity Strategy:**
    - Include clear policies and guidelines specific to OT and ICS security.
    - Integrate CNI protection into the broader national cybersecurity framework.
    - Address emerging threats and adapt the strategy to evolving technologies.
7. **Focus on Workforce Development and Expertise:**
    - Address the skills gap in cybersecurity, particularly in OT and ICS.
    - Implement training programs and incentives to retain cybersecurity talent.
    - Promote cybersecurity as a career path and support academic programs in this field.
8. **Leverage Technological Advancements:**
    - Adopt state-of-the-art cybersecurity technologies in OT environments.
    - Explore the use of AI and machine learning for threat detection and response.
    - Ensure secure integration of new technologies into existing OT systems.
9. **Improve Threat Intelligence and Information Sharing:**
    - Develop national platforms for sharing cyber threat intelligence.
    - Encourage proactive sharing of threat information among CNI operators.
    - Use shared intelligence to anticipate and respond to emerging cyber threats.

10. **Enhance Public Awareness and Education:**
    - Conduct national awareness campaigns on cybersecurity risks in OT and ICS.
    - Include cybersecurity education in school curricula and public programs.
    - Encourage community engagement in cybersecurity initiatives.

7.2 List of Hypotheses for New Zealand to Consider

The following hypotheses follow the same structure as is used above: each one provides a title, definition, rationale, considerations for implementation, and expected outcomes. As noted above, when considering the development or adoption and enforcement of cyber security standards for CNIs in New Zealand, policy makers, cyber security leaders, and the government of New Zealand may apply the learnings from this thesis both academically and pragmatically.

7.2.1 Hypothesis 1: Clear Definition and Framework for CNIs

- **Description:** If New Zealand clearly defines "nationally significant organisations" or "critical national infrastructure" as planned through the Emergency Management Bill or the DPMC consultation noted earlier in this thesis and establishes a comprehensive framework for cyber security measures, the management and protection of CNIs along with OT and ICS environments will be more effective and streamlined.
- **Rationale:** The success of Singapore's Cybersecurity Act in improving national security is due to the precise categorisation and obligations placed on CNIs, which leads to targeted risk management and effective use of resources.
- **Considerations for Implementation:** New Zealand should conduct a thorough analysis of Singapore's legislative framework, engaging with stakeholders across sectors to ensure a comprehensive approach that considers the unique aspects of New Zealand's infrastructure. It should use a partnership model to gather information from Five Eyes nations as well as Singapore and Estonia, and invite government experts to assist if required. Additionally, the government is encouraged to consider the following steps:
    - Engage in a cross-sector dialogue to agree upon what constitutes a CNI within New Zealand's unique context.
    - Draw from Singapore's legislative clarity and Estonia's strategic inclusiveness to ensure that all key infrastructure is considered and protected.

- Develop and disseminate comprehensive guidelines and standards that cater to the different categories of CNIs.

- **Expected Outcomes:**
    - A more streamlined approach to CNI protection with a shared understanding across government and industry.
    - Enhanced security protocols that are specific to the needs and risks of each category of CNI.
    - Better coordination and cooperation between CNIs and national cybersecurity efforts.

7.2.2 Hypothesis 2: Strengthen Public-Private Partnerships

- **Description:** If New Zealand fosters stronger public-private partnerships in its efforts to improve cybersecurity within CNIs, it will achieve a more comprehensive and effective defence against cyber threats.
- **Rationale:** The success of Estonia's collaboration with the private sector in cybersecurity has demonstrated the value of combining governmental oversight with private sector innovation and expertise. Singapore has similarly partnered with large technology companies to improve proactive threat intelligence sharing and incident response capabilities.
- **Considerations for Implementation:** Develop a national cybersecurity forum and incentivize private sector participation, taking cues from Estonia's model of public-private engagement. Consider largest gap areas within CNIs, especially for the cyber defence of OT and ICS environments, and prioritize capability development and strategic outcomes for such partnerships.
    - Create formal platforms for public-private cybersecurity collaboration, including regular forums and joint exercises.
    - Incentivize private sector participation through recognition programs, shared resources, and co-funding opportunities.
    - Encourage the sharing of threat intelligence and best practices between public and private entities, as is common in Estonia.
- **Expected Outcomes:** Increased innovation in cybersecurity solutions, capabilities, and a more cohesive national defence strategy against cyber threats. Some of the outcomes will emerge as follows:
    - A cohesive cybersecurity community with a shared mission to protect national interests.
    - Increased capacity to respond to and recover from cyber incidents due to a more diverse pool of expertise.
    - A culture of innovation in cybersecurity, leveraging insights from both sectors.

7.2.3 Hypothesis 3: Mandatory Standards and Reporting

- **Description:** If New Zealand enforces mandatory cybersecurity standards and incident reporting for CNIs and for any OT and ICS assets within CNIs, this will result in a more consistent adherence to security protocols and a proactive stance in cyber threat management.

- **Rationale:** The proactive security stance of Singapore's CNIs is largely to the result of mandatory compliance and reporting standards that ensure that organisations maintain a baseline level of cybersecurity. Most countries analysed as part of this thesis have mandated that CNIs report any cyber security incidents and have provided proper guidance to enable adoption of the reporting requirements. Currently in New Zealand, voluntary reporting and security standards are largely applied based on the inclination and limited resources of each CNI. Consequently, there is clearly a lack of visibility and neither the government nor the CNIs fully apprehend the size of the problem or the threat landscape.

- **Considerations for Implementation:** Implement mandatory cybersecurity standards and establish clear protocols for incident reporting, drawing from Singapore’s legislative model for CIIs. Enforcement can be gradual and based on an agreed order of priority depending on the definition of CNIs.

    - Study and adapt the key aspects of Singapore’s Cybersecurity Act, focusing on mandatory compliance requirements suitable for New Zealand's legal and corporate landscape.
    - Develop a comprehensive incident reporting system that balances transparency with confidentiality concerns.
    - Implement a phased rollout of mandatory standards, providing CNIs with guidance and support throughout the transition.
    - Create a dedicated body or governance structure or use regulatory constructs to manage and implement the requirements.

- **Expected Outcomes:** Improved cybersecurity across CNIs, with a unified and efficient incident response system. Better visibility and enhanced threat intelligence for the local threat landscape within New Zealand. The following benefits will emerge gradually:

- Consistent implementation of cybersecurity best practices across all CNIs.
- A collective advancement in the national cybersecurity posture.
- A more resilient national infrastructure with a reduced incidence of cyber breaches.

7.2.4 Hypothesis 4: Investment in Infrastructure and Talent

- **Description:** If New Zealand significantly increases its investment in cybersecurity governance, infrastructure, and talent, the country will enhance its defensive capabilities against cyber threats, particularly in OT and ICS environments.
- **Rationale:** Modelled after Estonia's investment strategy, this approach will not only enhance New Zealand's technological capabilities but also address the current skills gap within the cybersecurity sector, building a resilient foundation for future security needs.
- **Considerations for Implementation:** Allocate targeted funding for CNIs and especially for OT and ICS security education and infrastructure improvements, inspired by Estonia's commitment to cybersecurity funding. Additionally:
    - Equip forefront entities such as CERT and NCSC with better infrastructure investments so they can respond to incidents more effectively within CNIs.
    - Partner with educational institutions to create specialised programs that cater to the evolving needs of cybersecurity, particularly in OT and ICS.
    - Foster a culture of continuous professional development in cybersecurity, offering upskilling opportunities for current professionals.
- **Expected Outcomes:** A more robust cyber defence infrastructure and a well-equipped cybersecurity workforce in New Zealand with the following benefits:
    - A fortified cyber defence infrastructure equipped with the latest technologies.
    - A skilled and competent workforce capable of protecting and managing New Zealand's cybersecurity needs.
    - A sustainable and evolving cybersecurity ecosystem that keeps pace with global threats.

7.2.5 Hypothesis 5: Strategies for OT and ICS Protection

- **Description:** If New Zealand crafts and enforces focused strategies for the protection of OT and ICS environments, it will significantly reduce the cyber vulnerabilities inherent in these many critical and legacy systems.
- **Rationale:** Learning from Singapore's focused strategies on OT and ICS, New Zealand can mitigate the specific risks associated with these technologies, which are often distinct from traditional IT environments and require specialised security measures.
- **Considerations for Implementation:**
    - Conduct in-depth risk assessments specific to OT and ICS sectors, potentially collaborating with international bodies experienced in these fields.
    - Develop and implement OT and ICS security standards, drawing on the successful frameworks from Singapore and adapting them to New Zealand’s industrial context.
    - Create a task force dedicated to the protection of OT and ICS, involving experts from the private sector and academia.
- **Expected Outcomes:**
    - Enhanced security and resilience of New Zealand's OT and ICS.
    - Greater awareness and preparedness against the unique cyber threats faced by these systems.
    - Development of a skilled subset of cybersecurity professionals specializing in OT and ICS protection.

7.2.6 Hypothesis 6: Regulatory Compliance and Enforcement

- **Description:** If New Zealand strengthens its regulatory compliance and enforcement for cybersecurity across CNIs, this will then ensure a uniform security posture and mitigate the risk of systemic cyber threats.
- **Rationale:** Singapore's rigorous enforcement mechanisms have led to an improved cybersecurity landscape, serving as a model for how strict regulatory oversight can elevate the overall security posture of critical sectors. This hypothesis is critical to the success of hypothesis 3 related to enforcement reporting standards.
- **Considerations for Implementation:**
    - Benchmark against Singapore's regulatory environment to develop New Zealand-specific compliance guidelines and enforcement protocols.
    - Establish an independent body to oversee compliance, ensuring that CNIs adhere to the standards but without imposing undue burdens on them.
    - Incorporate flexible yet stringent measures that can adapt to the evolving cybersecurity landscape and threat vectors.
    - Develop clear guidelines on accountability for CNI leadership and boards of directors in relation to the adherence to cyber security standards.
- **Expected Outcomes:**
    - A standardised level of security across all CNIs, reducing the 'weakest link' vulnerabilities.
    - Increased accountability and improved cybersecurity practices within critical sectors.
    - A regulatory environment that supports a secure, reliable, and trustworthy national infrastructure.

7.2.7 Hypothesis 7: National Cybersecurity Strategy

- **Description:** If New Zealand develops and executes a comprehensive national cybersecurity strategy which explicitly highlights cyber security goals and aspirations for CNIs, its defence mechanisms will be bolstered against an array of cyber threats and its efforts will be aligned with its international peers.
- **Rationale:** In recent years Australia's well-defined national cybersecurity strategy has been pivotal in consolidating efforts and resources, providing a clear direction for the nation's cybersecurity initiatives. All of the nations reviewed in conjunction with this thesis reflect similar success when strategy is defined and communicated in a coherent manner.
- **Considerations for Implementation:**
    - Emulate Australia's strategy by integrating specific, measurable goals, dedicated resources, and a timeline for implementation.
    - Ensure that the strategy is dynamic and can evolve with changing cyber threats and technological advancements.
    - Foster a culture of cybersecurity that permeates all levels of government and business, encouraging proactive and preventive security measures.
- **Expected Outcomes:**
    - A cohesive and proactive national approach to cybersecurity.
    - Improved collaboration and coordination among government entities, businesses, and the cybersecurity community.
    - Alignment with international cybersecurity efforts, enhancing New Zealand's posture on the global stage.

7.2.8 Hypothesis 8: International Collaboration and Benchmarking

- **Description:** If New Zealand embraces international collaboration and adopts global benchmarking practices in cybersecurity, its cyber defence strategies will align with the world's best practices and it will avoid further delays and potential wasted resources.

- **Rationale:** The advancements in cybersecurity in the US and the UK, fuelled by international partnerships and benchmarking, display the benefits of global knowledge exchange and cooperation. By drawing on these advancements, New Zealand will also fill knowledge and capability gaps that may hinder it from achieving timely outcomes.

- **Considerations for Implementation:**

    - Establish formal partnerships for knowledge sharing with Singapore, Estonia, and the Five Eyes nations and establish working groups to achieve specific goals within a practical time.
    - Adopt benchmarking practices from leading cybersecurity nations to regularly assess and update New Zealand's cybersecurity measures.
    - Participate in international cyber exercises and adopt best practices in cybersecurity legislation and response strategies.

- **Expected Outcomes:**

    - Accelerated adoption of cutting-edge cybersecurity practices and technologies.
    - Enhanced capacity to predict, prevent, and respond to international cyber threats.
    - Recognition of New Zealand as a proactive and responsible member of the international cybersecurity community.

7.2.9 Hypothesis 9: Incident Response and Crisis Management

- **Description:** If New Zealand develops a dedicated national-level incident response and crisis management framework for CNIs, this will improve its readiness and effectiveness in managing cyber incidents.
- **Rationale:** Estonia's strategic incident response protocols, including its Red Team operations, have proven successful in improving the nation's cyber resilience. Singapore conducts nationwide cyber crisis management exercises, such as Exercise Cyber Star (XCS23), to improve crisis response capabilities and readiness against a wide range of cyber-attack scenarios on critical sectors using operational technology (OT) systems. Similarly, to enhance response readiness on an ongoing basis, the US and Canada regularly undertake GridEx, the largest grid security exercise in North America. .
- **Considerations for Implementation:**
    - Learn from Singapore, Canada, the US and Estonia’s proactive measures to establish various exercises capable of identifying and mitigating vulnerabilities before they are exploited.
    - Develop a national crisis management protocol, incorporating lessons from Estonia’s comprehensive approach to cyber threats.
    - Ensure that the crisis management framework is inclusive, involving stakeholders from various sectors to cover all aspects of national infrastructure.
- **Expected Outcomes:**
    - A robust capability to rapidly respond to and recover from cyber incidents, thereby minimizing their impact.
    - A culture of preparedness that anticipates potential cyber threats and has measures in place to address them efficiently.
    - Enhanced collaboration between government agencies, private sector entities, and international partners in response to cyber threats.

7.2.10 Hypothesis 10: Cybersecurity Awareness and Education

- **Description:** If New Zealand launches extensive cybersecurity awareness and education initiatives, this will foster a national culture of cybersecurity that enhances overall resilience to cyber threats across CNIs and beyond.
- **Rationale:** The comprehensive public awareness and educational campaigns in the UK have significantly improved the general population's understanding of cyber risks and best practices.
- **Considerations for Implementation:**
    - Implement a national awareness campaign that promotes cybersecurity best practices across different demographics, similar to the UK's strategy.
    - Integrate cybersecurity education into the national curriculum and professional development programs, ensuring that awareness is instilled at an early age and continues throughout one's career.
    - Incentivize businesses to invest in cybersecurity training for their employees, fostering a workplace culture that prioritizes cyber hygiene.
- **Expected Outcomes:**
    - A well-informed public that can identify and respond to cyber threats effectively.
    - Businesses that are more resilient to cyber-attacks because they have educated and vigilant employees.
    - A reduction in the overall risk of cyber incidents and their potential impact on New Zealand's national security.

8 Conclusion

In conclusion, this thesis has comprehensively examined New Zealand's current approach to securing its CNIs, focusing particularly on the complexities within OT and ICS environments. An in-depth analysis of New Zealand’s existing strategies, including the roles of the GCSB and NCSC, alongside a review of international practices from Five Eyes countries, Singapore, and Estonia, has helped identify shortcomings that New Zealand can consider for future efforts to enhance cybersecurity. The development of clear definitions and frameworks for CNIs, the strengthening of public-private partnerships, and the implementation of mandatory standards and reporting emerge as pivotal strategies. Additionally, the thesis highlights the need for significant investment in cybersecurity infrastructure and talent, coupled with the development of focused OT and ICS protection strategies, regulatory compliance, and a comprehensive national cybersecurity strategy. The thesis underscores the importance of international collaboration and benchmarking, robust incident response mechanisms, and heightened cybersecurity awareness and education. By integrating these insights and recommendations, New Zealand can elevate its cybersecurity posture, ensuring robust protection of its CNIs against evolving cyber threats. This proactive and informed approach is essential for safeguarding the nation’s critical infrastructure, ultimately contributing to its security, economic stability, and social welfare for the people of Aotearoa.

9 Citations:

DPMC New Zealand . (2023). *NEW ZEALAND'S NATIONAL SECURITY STRATEGY 2023-2028* . Wellington: New Zealand Government.

Hemsley, K. E. (2018). *History of Industrial Control System Cyber Incidents. United States.* Idaho National Lab. (INL), Idaho Falls, ID (United States).

10 References:

[i] Patrice Bock, Jean-Pierre Hauet, Romain Françoise, and Robert Foley. Lessons learned from a forensic analysis of the Ukrainian power grid cyberattack. ISA Interchange. Analysis of events during the year 2015 and 2016. https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware

[ii] Hemsley, K. E., & Fisher, R. E. (2018). History of Industrial Control System Cyber Incidents. Idaho National Laboratory. https://doi.org/10.2172/1505628

[iii] Brodt, O. (2023, October 16). *A brief history of ICS-tailored attacks*. A Brief History of ICS-Tailored Attacks. https://www.darkreading.com/attacks-breaches/brief-history-of-ics-tailored-attacks

[iv]ToI Staff. (2020, May 19). 6 facilities said hit in Iran's cyberattack on Israel's water system in April. The Times of Israel. https://www.timesofisrael.com/6-facilities-said-hit-in-irans-cyberattack-on-israels-water-system-in-april/

[v] Easterly, J., & Fanning, T. (2023, May 7). The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[vi] Carpenter, L., & Cano, N. (2023, May 22). The 2022 ICS/OT Vulnerability Briefing Recap. Dragos. https://www.dragos.com/threats/the-2022-ics-ot-vulnerability-briefing-recap/

[vii] Brubaker, N., Lunden, K., Proska, K., Umair, M., Zafra, D. K., Hildebrandt, C., & Caldwell, R. (2022, April 13). INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems. Mandiant. https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool

[viii] Wahlstrom, A., Roncone, G., Lunden, K., & Zafra, D. K. (2023, March 30). Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan. Mandiant. https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan

[ix] Sadowski, J., & Charrier, C. (2023, March 20). Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace. Mandiant. https://www.mandiant.com/resources/blog/zero-days-exploited-2022

[x] Carpenter, L., & Cano, N. (2023, May 22). The 2022 ICS/OT Vulnerability Briefing Recap. Dragos. https://www.dragos.com/threats/the-2022-ics-ot-vulnerability-briefing-recap/

[xi]Pullar-Strecker, T, (June 29, 2021), Ransomware attack: Waikato DHB supporting patients after documents dumped online https://www.stuff.co.nz/business/125592089/ransomware-attack-waikato-dhb-supporting-patients-after-documents-dumped-online

[xii]Anderson, R, (September 28, 2023), Auckland Transport experiencing another cyberattack, likely related to previous https://www.stuff.co.nz/national/crime/300980243/auckland-transport-experiencing-another-cyberattack-likely-related-to-previous

[xiii]RNZ. (2020, December 4). Scale of NZX cyberattacks 'unprecedented' in New Zealand - review. RNZ News. https://www.rnz.co.nz/news/business/432111/scale-of-nzx-cyberattacks-unprecedented-in-new-zealand-review

[xiv]CERT, New Zealand, (2023). Quarterly Report Highlights Q2 2023. CERT NZ. [PDF file]. https://www.cert.govt.nz/assets/Uploads/Quarterly-report/2023-q2/quarterly-report-highlights-q-2-2023.pdf

[xv] Microsoft New Zealand News Centre. (2023, March 8). Partnership announced to address urgent cybersecurity skills shortage. Microsoft New Zealand News Centre. https://news.microsoft.com/en-nz/2023/03/08/partnership-announced-to-address-urgent-cybersecurity-skills-shortage/

[xvi] Hill, M. (2023, October 31). Cyber security workforce shortage reaches 4 million despite significant recruitment drive. Reseller News. https://www.reseller.co.nz/article/709335/cyber-security-workforce-shortage-reaches-4-million-despite-significant-recruitment-drive/

[xvii]Adams, A. (2016, November 8). Cyber Security Skills Taskforce established. Beehive.govt.nz. https://www.beehive.govt.nz/release/cyber-security-skills-taskforce-established

[xviii]Walters, J. (2022, August 27). How government and industry can work together to address the cyber skills shortage. HRD New Zealand. https://www.hcamag.com/nz/specialisation/industrial-relations/how-government-and-industry-can-work-together-to-address-the-cyber-skills-shortage/418407

[xix] World Economic Forum. (2023). Global Security Outlook Report 2023. [PDF file]. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

[xx]New Zealand Defence Force. (2023). Defence Policy and Strategy Statement. [PDF file]. https://www.defence.govt.nz/assets/publication/file/23-0195-Defence-Policy-and-Strategy-Statement-WEB.PDF

[xxi]Department of the Prime Minister and Cabinet. (2023). National Security Strategy August 2023[PDF file].. https://www.dpmc.govt.nz/sites/default/files/2023-11/national-security-strategy-aug2023.pdf

[xxii] National Cyber Security Centre (New Zealand). (2022). Strategy 2024 [PDF file]. https://www.ncsc.govt.nz/assets/NCSC-Documents/Strategy-2024-PUBLIC-Version-Dec2022.pdf

[xxiii]Government Communications Security Bureau.(GCSB) (2023, August 31). New Zealand takes the first step in creating a lead operational cyber security agency. https://www.gcsb.govt.nz/news/new-zealand-takes-the-first-step-in-creating-a-lead-operational-cyber-security-agency/

[xxiv] Cybersecurity & Infrastructure Security Agency. (n.d.). Critical Infrastructure Sectors in the USA: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[xxv] National Protective Security Authority. (n.d.). Critical National Infrastructure, in the UK https://www.npsa.gov.uk/critical-national-infrastructure-0

[xxvi] Public Safety Canada. (2009). National Strategy for Critical Infrastructure [PDF file]. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

[xxvii] Australia. (2022). Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (C2022A00033). Federal Register of Legislation. https://www.legislation.gov.au/C2022A00033/latest/text

[xxviii] Department of the Prime Minister and Cabinet. (2023). DPMC Annual Report 2023. [PDF file] https://www.dpmc.govt.nz/sites/default/files/2023-11/dpmc-annual-report-2023-v2.pdf

[xxix] U.S. Department of Energy. (2022). C2M2 Version 2.1 June 2022 [PDF file]. https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf

[xxx] National Cyber Security Centre. (2024). About us. https://www.ncsc.govt.nz/about-us/

[xxxi] New Zealand Defence Force. (2023). Defence Policy and Strategy Statement. [PDF file]. https://www.defence.govt.nz/assets/publication/file/23-0195-Defence-Policy-and-Strategy-Statement-WEB.PDF

[xxxii]Department of the Prime Minister and Cabinet. (2023). National Security Strategy August 2023. [PDF file]. https://www.dpmc.govt.nz/sites/default/files/2023-11/national-security-strategy-aug2023.pdf

[xxxiii]National Cyber Security Centre (New Zealand). (2022). Strategy 2024 [PDF file]. https://www.ncsc.govt.nz/assets/NCSC-Documents/Strategy-2024-PUBLIC-Version-Dec2022.pdf

[xxxiv] New Zealand Information Security Manual. (n.d.). About the NZISM. https://nzism.gcsb.govt.nz/about-the-nzism

[xxxv] New Zealand Parliament. (2013). Telecommunications (Interception Capability and Security) Act 2013: https://www.legislation.govt.nz/act/public/2013/0091/latest/DLM5177923.html?src=qs

[xxxvi] National Cyber Security Centre and the Control Systems Security Information Exchange, (2019), Voluntary Cyber Security Standards for Control Systems Operators (VCSS-CSO), [PDF file]. https://www.ncsc.govt.nz/assets/NCSC-Documents/VCSS-CSO-Final-Oct-2019.pdf

[xxxvii] National Cyber Security Centre. (2024). Industrial control systems resources https://www.ncsc.govt.nz/resources/industrial-control-systems/

[xxxviii] New Zealand Parliament. (2023). Government Bill 2023/225. https://www.legislation.govt.nz/bill/government/2023/0225/8.0/LMS670569.html#d16197443e2

[xxxix]Department of the Prime Minister and Cabinet, New Zealand. (June 2023). Strengthening the Resilience of New Zealand's Critical Infrastructure System [PDF file]. https://consultation.dpmc.govt.nz/national-security-group/critical-infrastucture-phase-1-public-consultation/user_uploads/discussion-document--strengthening-the-resilience-of-nzs-ci-system.pdf

[xl]National Emergency Management Agency. (2023, September 15). 2023 Edition of the New Zealand Critical Infrastructure: A National Vulnerability Assessment. https://www.civildefence.govt.nz/resources/news-and-events/news-and-events/2023-edition-of-the-new-zealand-critical-infrastructure-a-national-vulnerability-assessment

[xli] National Cyber Security Centre (NCSC). (2023, July 12). 2022/2023 Cyber Threat Report (PDF file). https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf

[xlii] Defsec. (2023, June 20). Protecting New Zealand’s critical infrastructure from attack. https://defsec.net.nz/2023/06/20/protecting-new-zealands-critical-infrastructure/

[xliii] New Zealand Defence Force. (2021). Defence Assessment 2021. – emphasizing the important of a strong network of international security relationships, partnerships and alliances [PDF file] https://www.defence.govt.nz/assets/publication/file/Defence-Assessment-2021.pdf

[xliv] Department of the Prime Minister and Cabinet, New Zealand. (June 2023). Strengthening the Resilience of New Zealand's Critical Infrastructure System [PDF file]. https://consultation.dpmc.govt.nz/national-security-group/critical-infrastucture-phase-1-public-consultation/user_uploads/discussion-document--strengthening-the-resilience-of-nzs-ci-system.pdf

[xlv] Australia. (2022). Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (C2022A00033). Federal Register of Legislation. https://www.legislation.gov.au/C2022A00033/latest/text

[xlvi] Australian Government Department of Home Affairs. (2023, November 22). 2023-2030 Australian Cyber Security Strategy. [PDF file] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

[xlvii] Ibid, Shield 4, p 40

[xlviii] Australian Cyber Security Centre. (2023). ASD Cyber Threat Report July 2022 - June 2023. https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

[xlix] Australian Government Department of Home Affairs. (2023, November 22). 2023-2030 Australian Cyber Security Strategy. [PDF file] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

[l] RMIT University. (2023, November 22). Aussie tech breakthrough to protect critical infrastructure from cyber attacks. https://www.rmit.edu.au/news/all-news/2023/nov/tide-critical-infrastrcuture

[li] Australian Government Department of Home Affairs. (2023, November 22). 2023-2030 Australian Cyber Security Strategy. [PDF file] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

[lii]Canadian Centre for Cyber Security. (2023). National cyber threat assessment 2023-2024. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

[liii] Canadian Centre for Cyber Security. (2023). Home page. https://www.cyber.gc.ca/en https://www.cyber.gc.ca/en

[liv]Government of Canada. (2023). Chapter 5: Canada's leadership in the world. In Budget 2023. https://www.budget.canada.ca/2023/report-rapport/chap5-en.html

[lv]Université de Sherbrooke. (2023, February 23). The Université de Sherbrooke will contribute to the advancement of cybersecurity research in Canada. https://www.usherbrooke.ca/actualites/relations-medias/communiques/2023/fevrier/communiques-detail/49688

[lvi]Government of Canada, Department of Justice. (2023). Bill C-26: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c26_1.html

[lvii] UK Government. (2022). The NIS Regulations 2018. https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

[lviii]Information Commissioner's Office. (2021) The role of the National Cyber Security Centre (NCSC). https://ico.org.uk/for-organisations/the-guide-to-nis/the-role-of-the-national-cyber-security-centre-ncsc/

[lix] UK Government. (2022). Government Cyber Security Strategy. https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf

[lx] Jones, C. (2023, November 14). NCSC: UK must work harder to secure critical infrastructure. The Register. https://www.theregister.com/2023/11/14/ncsc_critical_national_infrastructure/

[lxi] National Cyber Security Centre. (n.d.). CNI regulation. https://www.ncsc.gov.uk/section/private-sector-cni/cni-regulation

[lxii] The White House. (2023, March 2). Fact sheet: Biden-Harris Administration announces National Cybersecurity Strategy. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[lxiii] National Security Agency. (2023, December 19). NSA publishes 2023 Cybersecurity Year in Review. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3621654/nsa-publishes-2023-cybersecurity-year-in-review/

[lxiv] Center for Strategic and International Studies. (2023, November 1). CISA Strategic Plan for 2023-2025: The Future of U.S. Cyber and Infrastructure Security. https://www.csis.org/analysis/cisa-strategic-plan-2023-2025-future-us-cyber-and-infrastructure-security

[lxv] The White House. (2023, March 2). Fact sheet: Biden-Harris Administration announces National Cybersecurity Strategy. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[lxvi] Ibid

[lxvii] Cyber Security Agency of Singapore. (2023, September 22). Nationwide Cyber Crisis Management Exercise to Test 11 Critical Sector's Response to Complex Cyber-attack Scenarios. https://www.csa.gov.sg/News-Events/Press-Releases/2023/nationwide-cyber-crisis-management-exercise-to-test-11-critical-sector-s-response-to-complex-cyber-attack-scenarios

[lxviii] Cyber Security Agency of Singapore. (2024, January 20). SingCERT. https://www.csa.gov.sg/Tips-Resource/Resources/singcert

[lxix] Cyber Security Agency of Singapore. (2023, September 29). CSA to Invest S$50 million to Uplift Talent, Innovation and Growth in Singapore's Cybersecurity Sector. https://www.csa.gov.sg/News-Events/Press-Releases/2023/csa-to-invest-50-million-to-uplift-talent-innovation-and-growth-in-singapore-s-cybersecurity-sector

[lxx] Cyber Security Agency of Singapore. (2023, October 17). CSA Collaborates with Microsoft and Google to Strengthen National Cyber Defence and Cybersecurity. https://www.csa.gov.sg/News-Events/Press-Releases/2023/csa-collaborates-with-microsoft-and-google-to-strengthen-national-cyber-defence-and-cybersecurity

[lxxi] Cyber Security Agency of Singapore. (2023, December 15). Public Consultation on the Proposed Cybersecurity (Amendment) Bill. https://www.csa.gov.sg/News-Events/Press-Releases/2023/public-consultation-on-the-proposed-cybersecurity-(amendment)-bill

[lxxii] Cyber Security Agency of Singapore. (2023). Advisory on the Secure Development and Provisioning of Distributed Ledger Technology (DLT)-Enabled Services. https://www.csa.gov.sg/Tips-Resource/publications/2023/advisory-on-the-secure-development-and-provisioning-of-distributed-ledger-technology-(dlt)-enabled-services

[lxxiii] Cyber Security Agency of Singapore. (2023, November 27). Guidelines for Secure AI System Development. https://www.csa.gov.sg/Tips-Resource/publications/2023/guidelines-for-secure-ai-system-development

[lxxiv] Government of Estonia. (2023, January 24). The Government Updated the National Security Concept of Estonia. https://www.valitsus.ee/en/news/government-updated-national-security-concept-estonia

[lxxv] BNS/TBT Staff. (2022, September 29). Estonian PM: State budget's focus is on security, supporting the population. The Baltic Times. https://www.baltictimes.com/estonian_pm__state_budget_s_focus_is_on_security__supporting_the_population/

[lxxvi] Government of Estonia. (2023, September 26). The government approved the state budget, which focuses on the security and sustainability. https://valitsus.ee/en/news/government-approved-state-budget-which-focuses-security-and-sustainability

[lxxvii] e-Estonia. (n.d.). e-Estonia Programme for Cyber Security. https://e-estonia.com/programme/cyber-security/

[lxxviii] Government of Estonia. (2023, January 24). The Government Updated the National Security Concept of Estonia. https://www.valitsus.ee/en/news/government-updated-national-security-concept-estonia