TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Nana Ueda

Japan's Cyber Defence:

A Cyber Power Theory Perspective

Master’s thesis

Technology Governance and Sustainability

Supervisor: Amirouche Moktefi

Tallinn 2024

I hereby declare that I have compiled the thesis independently
and all works, critical standpoints and data by other authors
have been properly referenced, and the same paper
has not been previously presented for grading.

The document length is 15,546 words, from the introduction to the end of the conclusion.

Nana Ueda, December.20.2024

Table of Contents

ABSTRACT

The author of this thesis has made an in-depth study of the Japanese cyber defence capability and its unique background through research on the Japanese constitution and laws, domestic government agencies responsible for cyber defence, and alliance with the United States (US) after World War II. In addition, through the lens of cyber power theory, a comparative case study on national strategies with countries that are reportedly successful in overcoming disadvantages and adversities in the real world was conducted. Specifically, two countries were selected for comparison: Estonia and South Korea. This thesis seeks to illuminate ways to promote the transformation of Japan's cyber defence capabilities and effectively enhance its cyber power by leveraging learnings from other countries in the process of examining the research questions.

Keywords: Japan, cyber defence capability, cyber power theory, national strategies, comparative case study, Estonia, South Korea.

List of Abbreviations

Acronym	Explanation
ACD	Active Cyber Defence
AI	Artificial Intelligence
C-TAS	Cyber Threat Analysis System
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CDU	Cyber Defence Unit
CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Response
CERT	Computer Emergency Response Team
CERT-EE	Estonian Computer Emergency Response Team
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CSH	Cybersecurity Strategic Headquarters
CyCon	Cyber Conflict
CYDF	Depertment of Cyber Defence
CYMAT	Cyber Incident Mobile Assistant Team
DDoS	Distributed Denial of Service
DEFCON	Defence Readiness Condition
EDL	Estonian Defence League
eGA	e-Governance Academy
EU	European Union
GCCD	Global Cybersecurity Center for Development
GDP	Gross domestic product
GDPR	General Data Protection Regulation

GHQ	General Headquarters of the Supreme Commander for the Allied Powers
ICT	Information and Communications Technology
ID	Identity Document
IISS	International Institute for Strategic Studies
ISACs	industry Information Sharing and Analysis Centers
IT	Information Technology
ITU	International Telecommunication Union
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
JSDF	Japan Self-Defence Forces
KDDI	Kokusai Denshin Denwa International
KISA	Korea Internet & Security Agency
KISC	Korea Internet Security Center
MIC	Ministry of Internal Affairs and Communications
MOC	Memorandum of Cooperation
MOD	Ministry of Defence (Japan)
NATO	North Atlantic Treaty Organization
NCSI	National Cyber Security Index
NDA	National Defence Academy
NICE	National Initiative for Cybersecurity Education
NIS	National Intelligence Service
NISC	National Center of Incident readiness and Strategy for Cybersecurity
NIST	National Institute of Standards and Technology
NPA	National Police AgencyRIA
NSA	National Security Agency
NSO	Office of National Security

NTT	Nippon Telegraph and Telephone Corporation
OECD	Organisation for Economic Cooperation and Development
PSIA	Public Security Intelligence Agency
R&D	Research and Development
RIA	Riigi Infosüsteemi Amet-Information System Authority
TalTech	Tallinn University of Technology
UK	United Kingdom
UN	United Nations
US	US

I. Introduction

The importance of cyber defence has accelerated globally over the past few decades, driven by unprecedented and rapid technological advances. Recent global developments, such as the war between Russia and Ukraine, tensions between China and Taiwan, North Korean provocations, and conflicts in the Middle East, have further underscored the urgency for nations to review and strengthen their cyber defence strategies. Japan, despite having the world's fourth-largest gross domestic product (GDP) and a wealth of talented engineers and technicians, has faced scrutiny regarding its cyber defence readiness. For example, Japan's perceived lag in cyber defence capabilities has been highlighted by experts like Cartan McLaughlin, founder of Nihon Cyber Defence, who suggests that Japan is 5 to 10 years behind countries like the US, the UK(United Kingdom) and other countries participating in Five Eyes, such as Australia, Canada, and New Zealand, in terms of cyber defence maturity (Asia Society, 2023). Furthermore, according to Matsumura, a Professor of International Politics and National Security, Japan does not have a comprehensive cyber strategy that utilises military, diplomatic, economic and other powers to counter cyber threats from a national security perspective. While the strategy and policy documents are quite substantial, there are still many issues to be addressed in terms of technical standards, the quality and quantity of personnel, organisational and system development, and budget scale. (Matsumura, 2022)

Indeed, looking back at the results of past global cyber defence capability surveys and the course of action taken in response to a recent high-profile cyber incident, it seems that McLaughlin and Matsumura have a point. The global cybersecurity index published by the International Telecommunication Union (ITU) in 2020, a trusted reference that measures a country's commitment to cybersecurity at the global level, ranked Japan 7th in the world, higher ranked than Five Eyes, with a balanced high score in each of the five pillars across cybersecurity commitments (ITU, 2020). It can be said that, at least until 2020, Japan's approach was regarded as on target and not at a pessimistic level internationally. However, the winds began to change around 2020. A study published by the International Institute for Strategic Studies (IISS) reported Japan is less capable in the security dimensions of cyberspace, despite its immense economic power, and grouped Japan in the lowest of the three tiers (IISS, 2021). In addition, the e-Governance Academy (eGA), an Estonian nonprofit foundation that assists public sector institutions worldwide in digital transformation, ranked Japan 52nd in the National Cyber Security Index (NCSI) as of 2023 (eGA, 2023). In addition to these, an event that disgracefully epitomises this reputation actually took place in Japan. In 2020, the US National Security Agency (NSA) discovered that Chinese military hackers had secretly accessed the Ministry of Foreign Affairs system of Japan for exchanging official telegrams containing sensitive diplomatic information. The NSA immediately notified the Japanese government to ask for a thorough investigation. Until that point, however, Japanese government officials had no clue what was going on or what needed to be done for that. That is mainly because, in fact, they were completely unaware of the malicious activities of the Chinese hackers on their networks. Shortly thereafter, Matt Pottinger, Deputy Assistant to the President, and Paul Nakasone, Director of the NSA visited Japan to share detailed information about the case and encourage them to improve vulnerable programs. Incidentally, this critical fact was made public by the American media a few years later, in 2023, and finally made known to the Japanese citizens. This series of events has caused great concern among the Japanese citizens. Not only because of the current state of Japan's cyber defence capability, but also the fact that the information was disclosed by the American media and the reluctance of the Japanese government to release the information for several years after the event. (Nakashima, 2023)

However, despite the fact that all of these indicators and events are sufficiently scrutinised and reliable, and it is acknowledged that there is still work to be done for Japan to catch up with the world's cyber powers, the scenario that Japan is falling far behind may be oversimplifying the complexity of Japan's cyber defence posture. Mihoko Matsubara, NTT (Nippon Telegraph and Telephone Corporation) Chief Cybersecurity Strategist, explained in the interview that the current situation in which the Japanese government and citizens are passively accepting the fact that they are being underestimated for various reasons and from biassed perspectives. There are actually several pieces of data that support this claim. First, there was the Tokyo Olympics and Paralympics, which were held during the coronavirus pandemic. There were reports in Europe and US that Japan might not be able to withstand intense cyber attacks, but as it turned out, despite the fact that there was more than double the number of cyber attacks than at the London Olympics, Japan was able to prevent all cyber attacks that could have interfered with the smooth running of the Games. This could be perceived as a landmark achievement. Although previous Olympic and Paralympic Games have also been targeted by cyber-attacks, Tokyo is the first to have successfully prevented any interference with the smooth running of the Games. (Matsubara, Yamaguchi and Koizumi, 2022) Moreover, according to a survey by global cyber security company Proofpoint, Japan is the country, out of the [1]15 countries surveyed, that pays the least ransomware ransoms. There are a number of possible reasons for this. Japan is a country that is prone to natural disasters, so the use of backups is widespread, and the high probability of being able to restore data, as well as the widespread social concept and moral values that one should not provide benefits to antisocial or criminal organisations. As a result of this attitude of not paying, it has been confirmed that the rate of ransomware infection itself has also decreased. In other words, launching attacks on specific companies or countries that are known not to pay ransom is not cost-effective for the attackers. Actually, the global infection rate for ransomware has increased by 5 points since last year to 69%, but the infection rate for ransomware in Japan has decreased by 30 points from 68% last year to 38%. (Sohta, 2024) Although these may also be partial aspects of a bigger picture, in light of Japan's unique position in the global cyber landscape, it is clear that simply mimicking the strategies of existing military and cyber superpowers will not suffice. Japan's path must be distinctive, aligning with its cultural values, historical context, and current political climate. The challenge lies in finding an approach that boosts Japan's cyber defence capabilities while staying true to its core identity as a nation dedicated to peace and technological

[1] US, UK, Australia, Spain, France, Germany, Japan, Canada, Italy, Brazil, South Korea, Netherlands, Singapore, Sweden, United Arab Emirates

innovation. This thesis explores how Japan can carve out its own space in the international cyber arena by strategically leveraging cyberspace to boost its international standing and confidence. By doing so, the author believes that Japan can overcome the limitations imposed by its physical constraints and historical commitments and effectively use cyberspace to achieve both security and influence in a manner uniquely fitting for the country.

1.1 Research Problem & Research Aim

Firstly, Japan’s cybersecurity activities have historically received minimal attention compared to the extensive scholarly and policy attention devoted to cyber superpowers like the US and China, highlighting the need for greater academic attention to Japan’s cyber capabilities, which remain limited in scope and volume (Kallender and Hughes, 2016). In particular, there is a relative lack of academic or political analysis from the perspective of exploring the use of soft power as well as hard power in cyberspace (Crandall and Allan, 2015). With this in mind, this thesis sets out two further main objectives. The first is to understand why Japan’s cyber defence capability remains behind, or is considered to be lagging behind, that of leading cyber nations by analysing its current situation. Secondly, to examine Japan's future strategic approach to cyber defence through comparative analysis with several countries that have succeeded in strategically utilising cyberspace to overcome disadvantageous conditions and adversity in the real world. Both analyses employ the ‘cyber power theory’ and the framework for evaluating national cyber defence capabilities derived from this theory.

1.2 Research Question

This thesis attempts to answer the following research questions:

- Is Japan really significantly behind in cyber defence? If so, what is the reason for Japan's alleged lag in cyber defence?
- How did the comparative countries use cyber power to overcome their disadvantages in the real world? What can Japan learn from them?

1.3 Structure of the Thesis

Firstly, to clarify the reasons why Japan is lagging behind in cyber defence, this author conducted research on current constraints such as the constitution, historical background, and government background. On that basis, it will apply the “Cyber Power Theory”, which provides a framework for evaluating a nation's capabilities in cyberspace, and examine Japan's strategic approach to cyber defence through comparative analysis with several countries that have succeeded in strategically utilising cyberspace to overcome disadvantageous conditions and adversity in the real world.

II. Literature Review

This chapter provides a comprehensive overview of the existing literature on cyberspace and cyber power. It begins by defining cyberspace, exploring its key characteristics. The chapter also examines the evolving concept of cyber power, and identifies the views of different authors on the components of cyber power. It then explores the role of active cyber defence (ACD) in cyber security strategy and examines how Japan's post-war pacifist identity and historical and social context influence its approach to cyber power and cyber diplomacy.

2.1 Cyberspace & Cyber Power

Cyberspace is a global domain of interconnected IT (Information technology) infrastructures, such as the Internet and telecommunications, that transcends physical boundaries to enable digital communication and data storage (Kuehl, 2009). The increasing significance of cyberspace in national security and international relations has led to the development of Cyber Power Theory, which examines how states leverage cyberspace to enhance their influence and strategic position. Rooted in traditional notions of power, the theory incorporates the unique aspects of cyberspace, where state and non-state actors engage in offensive, defensive, and strategic maneuvers. According to Joseph Nye, cyber power involves both soft power and hard power, with an emphasis on their strategic combination—smart power. Cyber power extends beyond offensive and defensive capabilities; it also includes the strategic use of information technology to shape global norms, influence events, and achieve national objectives, as shown in figure 1 and table 1 below.

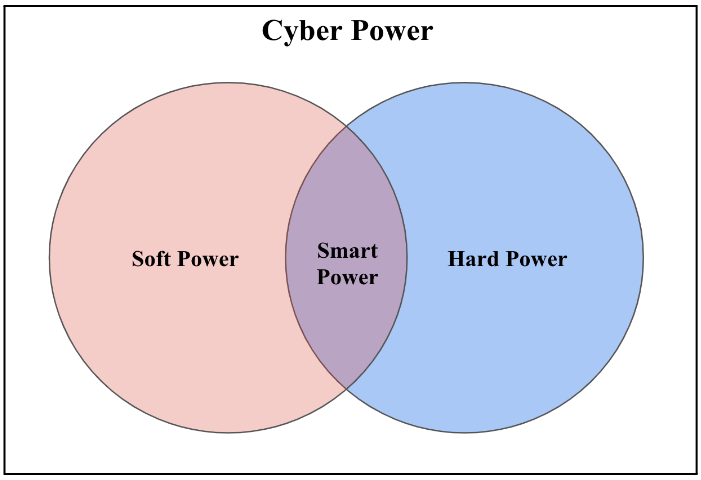

Figure 1. Cyber Power (Source: Nye, 2011)

Aspect	Soft Power	Hard Power	Smart Power
Nature	Attraction and influence through norms, culture, and trust	Coercion through offensive operations or economic measures	Strategic use of both soft and hard power
Tools	Norm advocacy, tech leadership, partnerships.	Cyberattacks, sanctions, retaliation.	Norm-building with credible deterrence.
Impact	Builds trust, global influence, and stability	Imposes costs, disrupts adversaries	Balances influence with enforcement

Table 1. Cyber Power Framework: Soft, Hard, and Smart Strategies (Source: Nye, 2011)

Kuehl defines cyber power as “the ability to use cyberspace to create advantages and influence events across all operational environments and instruments of power” (Kuehl, 2009). He highlights its role as a complement or alternative to traditional military power in an interconnected world. Haaster expands this by proposing a multidimensional framework, including technological capabilities, legal structures, societal resilience, and international norm-shaping, emphasizing both tangible and intangible factors like infrastructure, workforce, and political will (Haaster, 2016). Similarly, Rowland, Rice, and Shenoi identify offensive capabilities, defensive strategies, and intelligence operations as core elements, stressing the need for technological superiority and effective deterrence (Rowland, Rice, and Shenoi, 2014). In conclusion, cyber power is multifaceted, combining soft, hard, and smart power to achieve national objectives, shape international relations, and ensure security. Nations must adopt adaptive strategies to balance coercion, attraction, and integration in a contested global environment.

2.2 Global Trend: ACD

2.2.1 ACD

ACD is increasingly being discussed and adopted as a major trend in cybersecurity (Dewar, 2017). Unlike traditional passive defence, which focuses on strengthening systems and responding to attacks after they occur, ACD takes a proactive approach to countering cyber threats. Key elements include:

- Proactive Measures: Actively seeks out and disrupts potential threats before they cause damage, shifting cybersecurity from reactive responses to anticipatory engagement with adversaries.
- Threat Intelligence: Uses detailed intelligence on adversaries' tactics to enable preemptive risk mitigation.
- Adversary Engagement: Directly disrupts adversaries' operations or gathers intelligence through methods like decoy systems, deception, or legally bounded retaliation.

(Herpig, 2023)

Nations such as the US, the UK, and Australia have publicly indicated their intent to adopt ACD, highlighting its advantages over traditional passive defence. ACD deters adversaries by raising the risks and costs of malicious activities through immediate responses or retaliatory measures. However, ACD's proactive and potentially aggressive nature is not without controversy. Countries like Germany and Japan face challenges reconciling ACD practices with constitutional and normative constraints (Bendiek and Bund, 2023). Critics warn that preemptive and retaliatory actions could escalate cyber conflicts or provoke cyber wars, crossing ethical boundaries and violating international norms (Iasiello, 2023). From the perspective of international law, ACD raises questions about the limits of permissible "below-the-threshold" actions, as preemptive measures require precise intelligence and clear definitions of what constitutes a cyberattack and a justified countermeasure (Hathaway, 2014).

2.2.2 Balancing the Impact of ACD on Cyber Power

ACD reinforces national security by leveraging hard power through deterrence and retaliation against cyber threats, which requires advanced technical capabilities and cutting-edge technologies to execute effectively. Tools like AI (Artificial Intelligence)-driven threat detection, machine learning for predictive analytics, and quantum encryption are critical for ensuring precision and minimizing collateral damage. However, even with the most sophisticated technology, the aggressive nature of ACD carries inherent risks to soft power, which relies on trust, legitimacy, and ethical conduct. Precise and targeted operations may mitigate some risks, but overly coercive or unilateral actions can still alienate allies, harm a nation's reputation as a cooperative actor, and undermine its influence in shaping global cybersecurity norms. For nations like Japan, with a peace-oriented identity, these risks are especially pronounced, as aggressive ACD actions could erode diplomatic credibility and public trust if perceived as destabilizing or norm-violating. (Bendiek and Bund, 2023)

The responsible and effective implementation of ACD is crucial for achieving smart power—the strategic integration of hard and soft power. As mentioned above, while ACD strengthens hard power by enhancing deterrence and retaliation capabilities, overemphasis on this aspect risks undermining soft power, which is rooted in adherence to international norms and ethical principles. Therefore, nations must ensure that ACD operations align with these standards and actively contribute to the establishment of shared global cybersecurity rules, demonstrating their commitment to a secure and ethical cyberspace. Maintaining this balance requires transparent communication and public consensus, reinforcing the idea that ACD is fundamentally a defensive tool. By responsibly leveraging ACD within ethical and collaborative frameworks, nations can enhance their cybersecurity posture while building international trust. This approach not only solidifies their self-defence capabilities but also elevates their standing as reliable and principled actors in the global cyber environment, contributing to both national security and the development of a more secure international cyber landscape. (Kurosaki, 2023)

2.3 Post-WWII History of Japan

After WWII, Japan adopted the 1947 Peace Constitution, drafted under the guidance of the General Headquarters of the Supreme Commander for the Allied Powers (GHQ). This marked a shift from militarism to liberal democracy and pacifism (Katzenstein, 1996). The constitution's defining feature, Article 9, renounces war and prohibits maintaining military forces for offensive purposes, stating that war and the use of force are forever renounced as means of settling international disputes (The Government of Japan, 1947). While supported by many citizens, this reflected the GHQ's aim to prevent a resurgence of militarism. Subsequently, the San Francisco Peace Treaty and the Japan-US Security Treaty were signed in 1951. Although the San Francisco Peace Treaty brought sovereignty back to Japan, the Japan-US Security Treaty stipulated that the US would take the lead in Japan's security initiative and committed both countries to mutual defence in the event of an armed attack on Japan by stationing US troops in Japan. In 1954, amid the Cold War, after dialogue with the US, Japan decided to possess the Self-Defence Forces (JSDF). Subsequently, in 1978, the Guidelines for Military Cooperation between Japan and the US were formulated, establishing a framework for defence cooperation, disaster response, and joint training.

On its path to becoming a peaceful nation, Japan's reliance on the US security umbrella deepened, both psychologically and physically. Even after establishing the JSDF, Japan's dependency on US protection remained strong, with the absence of a fighting military force seen as a privilege that allowed Japan to avoid direct conflict. For the US, the Japan-US Security Treaty, signed during the Cold War, was strategically advantageous. It helped deter Soviet expansion in the Asia-Pacific region and solidified the liberal camp's position, making Japan an ideal geopolitical partner for the US to assert its leadership as the "Global Policeman" (Sakurada, 1998).

The region has remained tense, with China's military expansion and North Korea's missile provocations heightening diplomatic challenges. These developments sparked debates in Japan about taking greater responsibility for its national security and contributing actively to regional stability alongside the US. In 2015, Japan's parliament passed security legislation expanding the JSDF's roles, allowing limited collective self-defence and enhanced cooperation with allies. While adhering to the principles of Article 9, this marked a significant turning point for Japan's defence policy, leading to increased defence spending, equipment modernization, and the adoption of new systems (Mori, 2016; MOD (Ministry of Defence), 2019).

2.4 Japan's Soft Power in Diplomacy and Its Limitations

Japan has long utilized its cultural assets, such as anime, cuisine, and traditional performing arts, as a means of soft power to enhance its international image. According to Tsuneo Akaha, soft power's foundation lies in cultural appeal, political values, and foreign policy legitimacy. While Japan excels in leveraging its cultural soft power, its approach has limitations when applied to critical areas such as international security, particularly in cyberspace. The predominance of cultural elements—exemplified by initiatives like "Cool Japan"—has fostered a perception that Japan's global influence is largely confined to entertainment and consumer culture. This emphasis, while valuable in building goodwill, does not necessarily translate into the capacity to address pressing global challenges, such as those related to national and cyber security. (Akaha, 2005)

Japan's reliance on cultural soft power is deeply rooted in its postwar pacifist identity. Japan's post-World War II pacifist constitution, particularly Article 9, imposes constraints on its military capabilities, and as a result, diplomacy has focused primarily on cultural diplomacy, economic partnerships, and humanitarian aid. This pacifist stance, while promoting a peaceful international image, has resulted in Japan often taking a reactive rather than proactive role in global security matters. For instance, Japan's contributions to international security have largely focused on non-military, indirect involvement—such as financial contributions or humanitarian aid—rather than taking an active leadership role in shaping global norms or advocating for international security frameworks/solutions. (Funabashi, 2017)

Another limitation lies in the imbalance between Japan’s economic scale and its international influence. Despite being the world’s third-largest economy, Japan is often perceived as refraining from asserting its voice in global political and security matters. This disconnect between economic power and international influence highlights a lack of integration between Japan’s soft power and other forms of power, such as hard power or cyber power. (Fukushima, 2006) Nye emphasizes that soft power is most effective when paired with tangible capabilities that demonstrate a country’s ability to act on its values and objectives (Nye, 2004). In Japan’s case, the absence of a robust hard power or cyber power narrative dilutes the impact of its soft power in areas like international security.

III. Theoretical Framework

To comprehensively assess Japan's cyber defence capabilities and conduct a comparative analysis with other target countries, adopting a robust theoretical framework that provides a structured approach to evaluating national strategies is crucial. This thesis employs Cyber Power Theory, originally conceptualised by Joseph Nye and discussed by many other authors, as mentioned above, as the primary framework for analysis. This chapter, based on the concepts of Cyber Power Theory, provides a clear rationale for its adoption as the foundation of this study. Furthermore, the chapter will elaborate on how Cyber Power Theory's various dimensions apply to the comparative evaluation of national cyber defence capabilities.

3.1 Rationale for the Adoption of Cyber Power Theory

The adoption of Cyber Power Theory as the primary analytical framework in this study is justified by its comprehensive approach to understanding how states leverage cyberspace for strategic purposes. Cyber Power Theory provides a structured method to evaluate a nation’s cyber capabilities, focusing on both offensive and defensive dimensions, as well as its political and economic influence within the cyber domain. As cyberspace has become an increasingly significant arena for geopolitical competition, the theory's dual focus on hard and soft power offers valuable insights into national strategies in a digitally interconnected world. A key reason for adopting Cyber Power Theory is its ability to address not only traditional forms of power, such as military and economic might but also more nuanced forms of influence. Soft power, as conceptualised by Nye, is especially relevant in cyberspace, where the ability to shape global norms, foster international cooperation, and influence public opinion can be as important as offensive cyber capabilities. This is particularly crucial in a context where the effectiveness of traditional military force and economic sanctions is changing. According to Kim, the utility of military force and sanctions in cyberspace has become less straightforward, as cyber operations can circumvent conventional forms of coercion. (Kim, 2013) In this light, Cyber Power Theory provides a lens through which to evaluate how countries, including Japan, use non-coercive methods to project influence in cyberspace. Furthermore, social pressure plays an increasingly prominent role in the digital age. Kelley and Simmons argue that states can be influenced through social pressure, especially when international norms around cybersecurity are in flux. Nations with strong cyber capabilities can use social pressure to shape the behaviour of other states and actors in cyberspace, establishing themselves as leaders in setting global cybersecurity standards. (Kelley and Simmons, 2014) In addition to soft power, Cyber Power Theory's focus on hard power remains crucial, particularly when evaluating cyber attack and defence capabilities. Japan's development of cyber defensive measures and its growing attention to offensive capabilities within the context of national security make Cyber Power Theory a fitting framework. Moreover, the theory's ability to bridge the gap between technological aspects (e.g., cyber attack and defence capabilities) and political dimensions (e.g., international cooperation and legal frameworks) makes it a versatile and robust tool for understanding the complex dynamics of national cybersecurity strategies. This approach is crucial in an era where cyber threats are increasingly intertwined with geopolitical tensions and economic competition.

By employing Cyber Power Theory, this study benefits from a comprehensive framework that not only captures the technical aspects of cybersecurity but also accounts for the broader political, social, and economic contexts in which these cyber capabilities operate.

3.2 Five Key Dimensions of Cyber Power

With reference to the insights of Nye, Kuehl, and Haaster, this chapter will identify five key aspects of cyber power that are necessary for a comprehensive assessment of a nation's cyber defence capabilities. These five dimensions—cyber defence capabilities, cyber offensive capabilities, legal and policy frameworks, economic and political influence through cyber capabilities, and technological innovation and human capital—were developed by the author based on the conceptual foundations provided by these scholars. This section describes the derivation of each dimension, explaining how they contribute to a nation's overall cyber power.

1. **Cyber Defensive Capabilities**
    a) **Cybersecurity Infrastructure**: According to Nye, a country's ability to protect its digital infrastructure is essential to maintaining its sovereignty in cyberspace. Kuehl highlighted its role in preventing disruptions to critical systems like energy and finance, while strong defences deter attacks by raising costs for adversaries.

    b) **Incident Response and Recovery**: Haaster emphasized the importance of rapid response and recovery, as no defence is perfect. A well-trained Cyber Incident Response Team (CIRT) can contain damage and restore operations, showcasing resilience and defensive strength.

2. **Cyber Offensive Capabilities**
    a) **Cyber Attack Capabilities:** Cyber attack capabilities are directly connected to ACD as they enable a proactive stance in mitigating threats and deterring adversaries. Kuehl noted that offensive cyber operations, such as preemptive attacks on critical infrastructure, provide strategic leverage and deterrence. Nye emphasized that these capabilities can influence global events by disrupting adversaries' operations, but their effectiveness relies on surprise and careful calibration.

    b) **Cyber Intelligence and Espionage:** Intelligence gathering and espionage are indispensable components of ACD, as they provide the situational awareness needed to execute both defensive and offensive actions effectively. Nye underscores that collecting information in cyberspace enhances a nation's decision-making processes and strengthens its ability to anticipate and counter threats. In the context of ACD, intelligence capabilities are directly tied to the success of preemptive actions, enabling nations to disrupt adversaries before they can launch attacks. Haaster adds that cyber espionage allows a nation to evaluate its adversaries' capabilities and intentions, providing vital insights for strategic planning. Within ACD, this intelligence feeds into broader information warfare strategies, where the boundaries between espionage and influence operations often blur. The integration of cyber intelligence with attack capabilities ensures that ACD not only responds to immediate threats but also disrupts adversaries' long-term plans, solidifying a nation's cyber resilience and strategic position.

3. **Legal and Policy Frameworks**

   a) **National Cybersecurity Policies**: According to Nye, coherent and comprehensive national cybersecurity policies form the foundation for cyber governance. These policies define the roles and responsibilities of various actors, both public and private, in securing cyberspace. Kuehl emphasised that a strong legal framework not only ensures internal coordination but also enables the government to hold entities accountable, promoting the development of robust cybersecurity capabilities. Well-structured policies, such as those governing data protection and cybercrime, enhance national security and reinforce cyber power.

   b) **International Cooperation**: Haaster underscores the importance of international legal cooperation in cyber defence. Countries that engage in multilateral agreements, participate in global cybersecurity forums, and contribute to setting international standards strengthen their global influence in cyberspace. This form of soft power, described by Nye, allows nations to shape the rules of engagement in cyberspace and build trust among international partners. Nations with strong international ties in cybersecurity, such as Japan's involvement in global cyber norms, extend their influence beyond their borders.

4. **Economic and Political Influence through Cyber Capabilities**

   a) **Cyber-Related Economic Strength**: Nye posited that economic power in the digital age is deeply tied to cyber technologies. Countries that lead in cyber innovation, digital infrastructure, and the cybersecurity market wield significant economic power in global markets. Haaster explains that a nation's cyber power is directly linked to its ability to harness digital technologies for economic growth, which, in turn, strengthens its international influence.

b) **Information Dominance**: Information is a key asset in the cyber domain. Nye argued that nations that can control and manipulate information flows have a distinct advantage in international relations, as information campaigns can influence global narratives. Kuehl further elaborated that information dominance allows states to project soft power by shaping perceptions, controlling media narratives, and influencing both domestic and foreign populations. This strategic use of information can play a critical role in advancing a nation's geopolitical goals.

5. Technological Innovation and Human Capital

a) **Cyber Workforce Development**: Nye highlights that human capital is a core component of a nation's cyber power. Nations that invest in cybersecurity education, training, and workforce development can cultivate a pool of highly skilled professionals capable of defending and advancing the nation's interests in cyberspace. Haaster stressed the importance of cultivating human capital in both technical skills and strategic thinking to ensure long-term resilience and leadership in cyber defence. A nation's cyber workforce is an enduring asset, and the ability to continuously train and innovate is crucial for maintaining cyber power.

b) **Investment in Cybersecurity Research and Development (R&D)**: Kuehl pointed out that investment in R&D is essential for a nation to remain competitive in cyberspace. Nations that prioritise R&D can develop cutting-edge technologies that enhance their offensive and defensive capabilities. Haaster supported this by noting that technological innovation is a crucial factor in maintaining a competitive edge in cyberspace. Countries with a strong focus on R&D are more likely to produce novel cyber capabilities and defend against emerging threats.

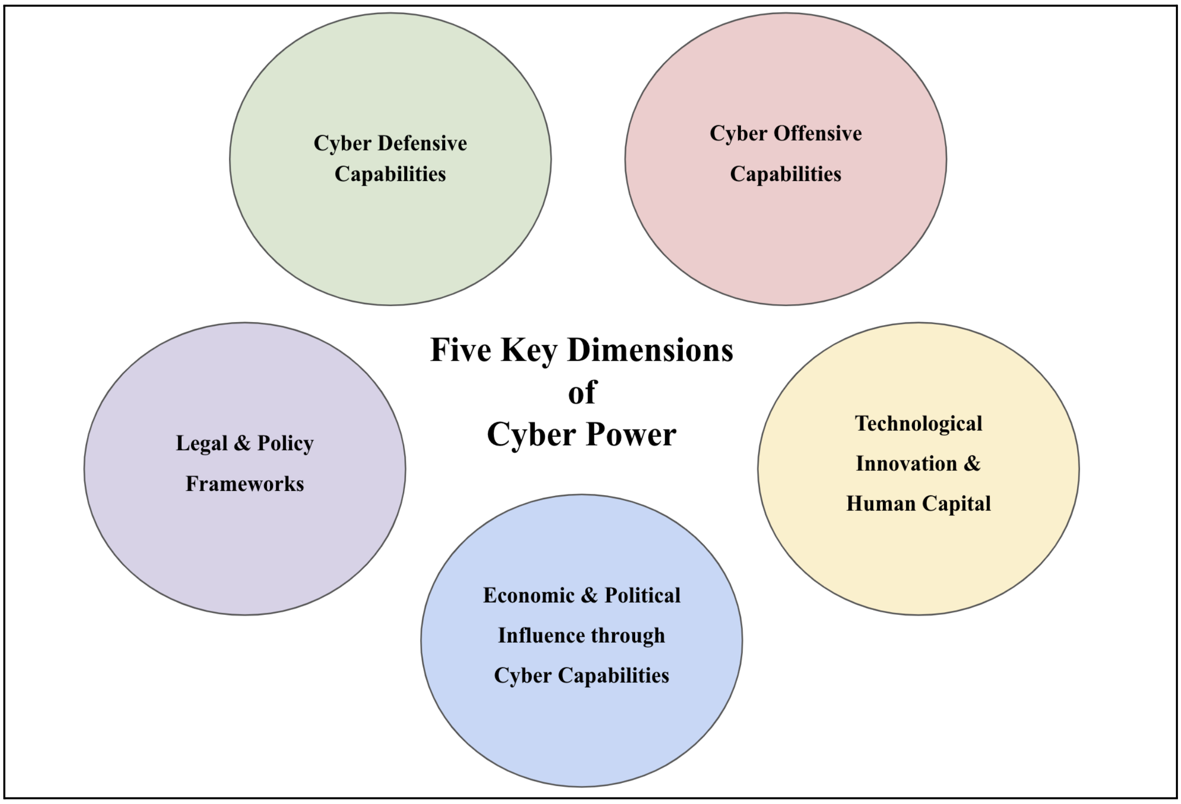
Cyber Defensive Capabilities
Cyber Offensive Capabilities
Five Key Dimensions of Cyber Power
Legal & Policy Frameworks
Technological Innovation & Human Capital
Economic & Political Influence through Cyber Capabilities

Figure 2. Five Key Dimensions of Cyber Power

IV. Research Methods

4.1 Research Design & Strategy

This thesis adopts a qualitative research approach, particularly suited for understanding complex phenomena such as national cyber defence strategies. The decision to use qualitative methods is based on several key factors. First, the nature of the research problem involves exploring dynamic events and policies over which the researcher has no direct control. This makes experimental or purely quantitative methods less applicable (Yin, 2009). Second, cyber defence strategies are shaped by a multitude of cultural, geopolitical, and technological factors, each influenced by context-specific conditions that cannot be easily quantified or reduced to statistical analysis alone. For example, the geopolitical tensions between states, national security imperatives, and differences in technological development require a deep understanding of each country's unique circumstances. Qualitative research allows for a nuanced exploration of these factors, accommodating the complexity of national cyber strategies and their various dimensions. Qualitative research is inherently exploratory, aiming to investigate the 'how' and 'why' behind social events or phenomena, rather than simply measuring their occurrence. (Polkinghorne, 2005) Finally, qualitative research is particularly valuable for studying cyber defence, a field where universal solutions are not readily available. As cyber defence strategies continuously evolve and lack universally agreed-upon methods, qualitative inquiry facilitates an open-ended investigation into various national approaches and the contextual factors influencing these strategies. (Creswell, 2013; Merriam, 2009)

4.2 Case Selection

The comparative countries, Estonia and South Korea, were selected for their internationally recognized success in leveraging cyberspace strategically and overcoming real-world adversities. Below is a summary of the key characteristics supporting this choice.

[Estonia]

- Estonia is a global leader in cybersecurity, known for its advanced cyber defence policies and role as an international norm entrepreneur. It hosts NATO (North Atlantic Treaty Organization) CCDCOE (Cooperative Cyber Defence Centre of Excellence) in Tallinn (CCDCOE, 2023).
- In response to the 2007 cyberattack and ongoing geopolitical threats, Estonia developed resilient cyber infrastructure, pioneering e-governance and robust cyber defence policies to safeguard national security (RIA, 2020).

[South Korea]

- South Korea ranks first in cyber defence capabilities in Asia, especially in the development of a phased ACD approach (ITU, 2020).
- Facing a declining birth rate and labor shortages, South Korea increasingly utilises on AI technology and automation to maintain productivity and address economic challenges (Valeriano and Leasure, 2024).

4.3 Data Collection and Analysis Methodology

The data for this research were collected through an extensive review of publicly available primary sources and secondary sources, and personal interview that were accessible on the internet at the time of writing. Primary sources in this context refer to official documents in each nation or related international organisations, such as cyber defence/information security strategies and associated actions/execution plans, digital transformation strategies, foreign policies, national security strategies, military/defence strategies, R&D policies/plans, education systems/projects. Secondary sources in this context include official reports, assessments, press releases, and similar third-party accounts published by reliable sources. For both sources, data were collected in English and Japanese, however, official English translations of the documents were used for citations when available. In cases where such translations were not available, the DeepL translation was used. To avoid the possibility of inaccuracies due to machine translation, each document was visually compared to the original; minor nuance errors were corrected by the author and, where necessary, confirmed by cross-checking with other official English-language sources. The primary source data collection process adhered to the principle that each document must be valid. For this thesis, documents were considered valid as long as they were available on official web pages and had not been replaced by a successor strategy, policy, and so forth. For personal interview, it was conducted with Kozo Nakatani, Director of Taiwanese security company Cycraft, who is an expert in the field of global cybersecurity, digital strategy to gain qualitative insights and validate findings from the document review.

Each country presents unique attributes in terms of international standing, strategic priorities, and its definition and approach to “Cyber Defence.” Therefore, a direct application or imitation of a cyber defence framework from one country to another may not yield effective results. Instead, this thesis aims to distil best practices that Japan can adapt to its specific context, with particular emphasis on soft power and innovative cyber policies. The capability analysis and comparative case study are based on five main dimensions: cyber defensive capabilities, cyber attack capabilities, legal and policy frameworks, economic and political influence through cyber power, and technological innovation and human capital. These dimensions provide a comprehensive framework for analysis by covering the full spectrum of factors that contribute to national cyber power. Each dimension offers a lens through which to evaluate key aspects of a country’s cyber strategy: defensive and offensive capabilities assess a country’s resilience and response potential; legal and policy frameworks ensure alignment with national and international laws; economic and political influence highlights the role of cyber power in extending global influence; and technological innovation and human capital address the critical infrastructure and skills needed for sustainable cyber growth. The analysis includes Estonia and South Korea as comparative case studies, each exemplifying successful approaches to cyber defence that effectively enhance national cyber power despite geographical and geopolitical limitations. Both countries have strategically developed their cyber power to overcome physical and regional challenges. This multidimensional approach enables a nuanced understanding of these countries' successes, ensuring that recommendations for Japan are relevant, implementable, and context-sensitive.

4.4 Limitations and Challenges

As Yin explains, case studies are intended to generalise theoretical propositions rather than entire populations or universes. While the findings in this thesis offer meaningful insights, they may not be easily transferable to other countries that, despite certain parallels with Japan, possess unique characteristics. (Yin, 2018) Additionally, as Eisenhardt points out, data on complex issues like national cyber defence capabilities is often disclosed inconsistently. Each country's standards of confidentiality differ, making it challenging to perform a standardised analysis across multiple nations. (Eisenhardt, 1989) Furthermore, case study methods have inherent limitations, particularly in assessing the frequency or representativeness of particular events and in estimating the "causal weight" of variables (Bennett, 2004). Power—cyber or otherwise—derives significance from interactions and comparisons, as it is shaped through negotiations and relationships with other nations. Finally, an added challenge is the potential subjectivity of rankings and evaluations on cyber power, as metrics and methodologies used by research organisations can vary and may lack transparency (Kim, 2013).

In order to overcome these challenges, in the process of gathering data and information, the author followed the approach of Creswell and Eisenhardt, and examined data and information from various sources in multiple countries, seeking supporting evidence wherever possible. For example, the author emphasised the use of multiple data sources, including not only academic journal articles and research reports, but also interviews with relevant parties, videos, and archived data. In this way, we tried to minimise any potentially biassed or subjective opinions and maintain a neutral perspective. (Creswell, 2013; Eisenhardt, 1989)

V. Analysis By Framework Application

5.1 Japan

1. Cyber Defensive Capabilities

a) **Cybersecurity Infrastructure**: Japan's cybersecurity infrastructure is anchored in the Basic Act on Cybersecurity, which provides a comprehensive legal framework that underpins the national cybersecurity strategy, protection of critical infrastructure, and public-private sector cooperation. Key governmental agencies with cybersecurity roles are organised across three primary areas.

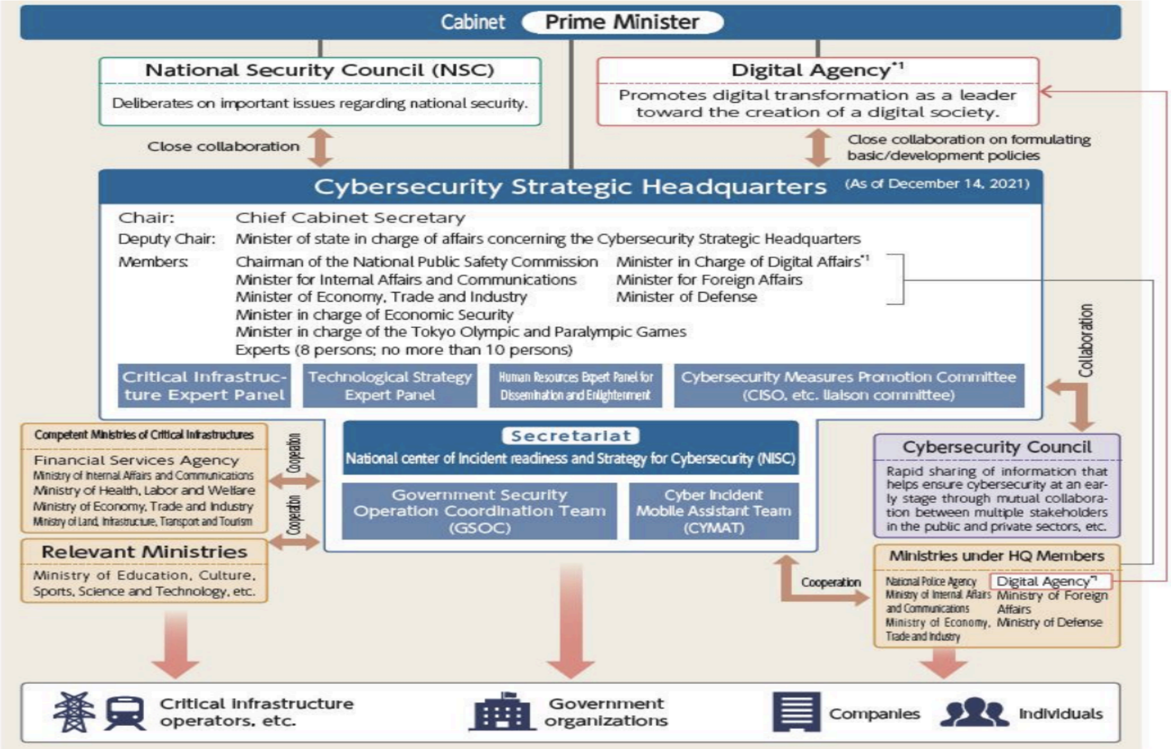
Cabinet
Prime Minister
National Security Council (NSC)
Deliberates on important issues regarding national security.
Digital Agency*1
Promotes digital transformation as a leader toward the creation of a digital society.
Close collaboration
Close collaboration on formulating basic/development policies
Cybersecurity Strategic Headquarters
(As of December 14, 2021)
Chair: Chief Cabinet Secretary
Deputy Chair: Minister of state in charge of affairs concerning the Cybersecurity Strategic Headquarters
Members: Chairman of the National Public Safety Commission
Minister for Internal Affairs and Communications
Minister of Economy, Trade and Industry
Minister in charge of Economic Security
Minister in charge of the Tokyo Olympic and Paralympic Games
Experts (8 persons; no more than 10 persons)
Minister in Charge of Digital Affairs*1
Minister for Foreign Affairs
Minister of Defense
Critical Infrastructure Expert Panel
Technological Strategy Expert Panel
Human Resources Expert Panel for Dissemination and Enlightenment
Cybersecurity Measures Promotion Committee (CISO, etc. liaison committee)
Collaboration
Competent Ministries of Critical Infrastructures
Financial Services Agency
Ministry of Internal Affairs and Communications
Ministry of Health, Labor and Welfare
Ministry of Economy, Trade and Industry
Ministry of Land, Infrastructure, Transport and Tourism
Cooperation
Cooperation
Relevant Ministries
Ministry of Education, Culture, Sports, Science and Technology, etc.
Secretariat
National center of Incident readiness and Strategy for Cybersecurity (NISC)
Government Security Operation Coordination Team (GSOC)
Cyber Incident Mobile Assistant Team (CYMAT)
Cybersecurity Council
Rapid sharing of information that helps ensure cybersecurity at an early stage through mutual collaboration between multiple stakeholders in the public and private sectors, etc.
Cooperation
Ministries under HQ Members
National Police Agency
Ministry of Internal Affairs and Communications
Ministry of Economy, Trade and Industry
Digital Agency*1
Ministry of Foreign Affairs
Ministry of Defense
Critical infrastructure operators, etc.
Government organizations
Companies
Individuals

Figure 3. Implementation framework of public entities involved in cyber defence of Japan

(Source: NISC, n.d.)

First, agencies under the direct authority of the Cabinet Office, including the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and the Cybersecurity Strategic Headquarters (CSH), focus on policy development and strategic coordination. The CSH leads national cyber policy formulation, with support from NISC and the Cybersecurity Council, which facilitate secure information sharing and collaboration between government entities and the private sector. Additionally, sector-specific bodies, such as CEPTOAR, provide critical infrastructure providers with a platform to share threat intelligence and independently coordinate defensive measures (The Government of Japan, 2018; NISC, 2022). Second, JSDF operates dedicated cybersecurity units to secure and defend the information and communication systems of MOD and JSDF. Finally, the National Police Agency (NPA) and the Public Security Intelligence Agency (PSIA) have specialised units focused on countering cybercrime, mitigating cyberterrorism risks, and safeguarding public security within the cyber domain.

Although Japan's cybersecurity framework aims to establish public-private cooperation across various fields and appears comprehensive, it faces significant challenges. According to Matsumura, Japan's cybersecurity structure suffers from a fragmented, “stove-piped” organisation that limits interagency integration and creates jurisdictional barriers. The NISC functions merely as a liaison and coordination body, with no single ministry or agency tasked with comprehensive cyber crisis management. Instead, responsibilities are divided among different agencies: the Ministry of Internal Affairs and Communications (MIC) manages the information and communications sector, the Ministry of Economy, Trade and Industry oversees critical infrastructure, and the NPA addresses cybercrime and cyberterrorism related to critical infrastructure. This separation perpetuates a siloed structure, obstructing efficient national coordination in cybersecurity. (Matsumura, 2022) Furthermore, Jinnai expressed concern over the unclear division of roles between government ministries and agencies in the cyber domain. In particular, despite the fact that the JSDF has the potential to play a central role in national security, its duties and authority in cyberspace remain unclear. Legal and institutional discussions regarding the

JSDF's role in cyberspace have not progressed sufficiently, and as a result, many uncertainties remain in Japan's cyber defence system. (Jinnai, 2024)

b) **Incident Response and Recovery**: Incident response in Japan is managed through a structured network involving multiple government and specialised agencies. NISC coordinates cross-agency collaboration and provides technical support through entities like the Cyber Incident Mobile Assistant Team (CYMAT), which assists in incident containment, recovery, and analysis. JSDF Cyber Defence Unit (CDU) also plays a role in incident response, focusing on cyber defence across military domains and collaborating with other national agencies and international partners. Despite these efforts, Japan's incident response system faces challenges, including fragmented reporting structures and limited real-time intelligence capabilities due to constitutional restrictions on monitoring communications. (Uesugi and Hirayama, 2018; MOD, 2022)

One critical area for improvement lies in the activities of industry Information Sharing and Analysis Centers (ISACs), which currently lack the robust interaction necessary for effective information exchange. In Japan, the legacy of the lifetime employment system in the private sector has resulted in relatively little human mobility and even less mobility between the public and private sectors (Nishimura, Ikeda and Tagami, 2023). Furthermore, a significant obstacle to information sharing lies in the reluctance of private companies to report or share cybersecurity incident details due to concerns about data leakage and the reputational risks associated with such disclosures (Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), 2021). The lack of human resource mobility, the immaturity of ensuring privacy on information sharing and guidelines for disclosure of cybercrime victimisation hinder the formation of networks between organisations and across industries and prevent the active exchange of ideas and expertise that is essential for effective incident response.

Finally, a key issue within Japan's public sector is the lack of leadership at the managerial level, particularly individuals with military or cybersecurity expertise. Although Japan’s absence of an official military or conscription system limits the development of broadly trained personnel, this alone does not account for the gap. The reliance on a bottom-up approach may suffice during peacetime but falls short in crisis situations requiring decisive top-down command. (Nakatani, 2024)

2. Cyber Offensive Capabilities

a) **Cyber Attack Capabilities**: Japan reinterpreted Article 9 in 2015, allowing for the limited exercise of the right to collective self-defence. However, the article is still one of the major stumbling blocks. Furthermore, the development of offensive cyber capabilities is a sensitive political issue that has as much impact on international relations as it does in the traditional military domain. For example, Japan was and remains heavily dependent on the US security umbrella. (Matsumura, 2022)

In this context, special consideration should be given not only to the relationship and power balance between Japan and the US, but also to relations with South Korea and China, which have close historical ties, and other cooperating countries in Asia. (Hoshiyama, 2008) Given the above reasons, Japan would continuously take a cautious approach to building and exercising offensive cyber capabilities. (Matsubara, Yamaguchi and Koizumi, 2022) However, this cautious stance, deeply rooted in Japan's pacifist identity, may serve as an opportunity to enhance its soft power. By maintaining pride in its peace-oriented approach, Japan can position itself as a leader in ethical cyber governance and diplomacy. This aligns with the global demand for rules and norms in cyberspace, where Japan's advocacy for stability, cooperation, and restraint could resonate strongly. It could also contribute to trust-building with emerging nations and neutral actors in the international arena.

In light of this, a full-fledged discussion on the definition of ACD within Japan and the building of public consensus is urgently needed. This should include considerations of how Japan can balance its pacifist principles with the demands of modern cybersecurity. At present, this has not yet begun as a serious initiative in the Diet, but Russia's invasion of Ukraine and the growing tensions between China and Taiwan will call for more urgent and active debate. Importantly, Japan can use this opportunity not only to reassess its policies but also to lead by example, championing a model of cyber resilience and defence that prioritizes ethical principles and cooperative engagement over purely offensive strategies.

b) **Cyber Intelligence and Espionage**: In addition to the Constitution of Japan containing Article 9, Japan has Article 21(2), “Secrecy of Communications and Prohibition of Censorship”. This article limits the government's ability to conduct real-time monitoring and data collection, complicating efforts to proactively gather intelligence on cyber threats. Consequently, Japan must carefully balance its intelligence operations with constitutional protections on privacy and freedom from censorship, impacting the scope of its cyber intelligence and espionage initiatives. (Matsumura, 2022)

Moreover, Japan relies heavily on foreign-developed cybersecurity tools due to insufficient domestic R&D, limiting its ability to create tailored tools and intelligence for its unique needs. This dependence not only poses potential security risks but also undermines efforts to establish independent intelligence capabilities (Inoue, n.d.). To bridge this gap, Japan is expanding international cybersecurity cooperation but must address challenges such as integrating cybersecurity with military strategy, historical contexts, and multilingual capabilities (Matsubara, 2022). Multidisciplinary teams spanning government, private sectors, and academia are needed to address issues like wiper malware, DDoS (Distributed Denial of Service) attacks, intelligence, and international law. These teams require both tactical expertise for immediate threats and strategic foresight for long-term policies. By fostering diverse talent and global strategic roles, Japan can fortify its cybersecurity foundation (Matsubara, Yamaguchi, and Koizumi, 2022).

3. Legal and Policy Frameworks

a) **National Cybersecurity Policies**: The Basic Act on Cybersecurity, enacted in 2015, establishes fundamental principles, clarifies government responsibilities, and provides a framework for cybersecurity initiatives. It mandates the development of a comprehensive national cybersecurity strategy, emphasizes the protection of critical infrastructure and information assets, promotes education and awareness, and fosters cooperation between the government and private sector. As seen in Articles 6 and 7 of the law, a unique aspect is Japan's reliance on the independent initiatives of critical infrastructure providers rather than direct government mandates, reflecting a collaborative approach. (The Government of Japan, 2018) Just as the NCSI rated the development of Japan’s cybersecurity policy with a perfect score, it is safe to say that the Japanese government’s policies and strategies are comprehensive, well thought-out, and far-reaching (eGA, 2023). Of course, there are many areas that could be called still in the process of development. For example, the argument is maturing that, at least for critical infrastructures, the government should not only rely on the autonomy of the private sector but also establish a system that justifies incident reporting obligation and direct supervision. (Yamaguchi, 2019) Currently, reporting obligations with a fine or penalty only apply to cases where a personal data breach has occurred, and this has only started in 2022 (The Cabinet Office of Japan, 2022).

b) **International Cooperation**: Japan’s efforts to strengthen international cooperation in cybersecurity extend across various regions and partnerships. Its relationship with the US and NATO remains central to its strategy, while Japan also seeks to broaden its international presence beyond traditional alliances. In diplomacy with a view to Japan's security, developing cooperative relationships with various countries across continents would be extremely important in order to strike a balance between soft and hard power. In 2012, the Internet Threat Monitoring System "TSUBAME" was released primarily by the National Institute of Information and Communications Technology, a Japanese research organisation, which has been observing various scanning activities in the Asia-Pacific region since (JPCERT/CC, 2012). Moreover, in April 2021, the MOD and JSDF team was formed to officially participate in the "Locked Shield" exercise for the first time (MOD, 2021). Japan's cybersecurity contributions remain underrecognized globally. However, Matsubara, highlights the need for Japan to proactively showcase its expertise and initiatives internationally, particularly through English communication, to enhance visibility and foster global partnerships in R&D (Matsubara, 2022). This challenge reflects broader limitations in Japan's public diplomacy, which plays a vital role in shaping regional and global orders while enhancing national soft power. Factors such as insular media, historical disputes with neighboring countries, however, and sensitivity to US pressures hinder Japan's strategic messaging on security and digital policies. (Hoshiyama, 2008) Despite its substantial cultural soft power, Japan has struggled to extend this influence to cybersecurity and digital diplomacy. To establish itself as a stabilizing force in the global society and a key actor in global cyber governance, Japan must strategically align its cultural soft power with its contributions to cybersecurity.

4. Economic and Political Influence through Cyber Capabilities

a) **Cyber-Related Economic Strength**: Japan has suffered from the economic stagnation known as the "lost 30 years". Thus, the cyber industry has also been driven by the trend of reducing R&D investment and minimising business risks. (Vosse, 2024) As Bartlett stated, the Japanese IT industry is no exception and has been focused on releasing 'good' code rather than 'innovative' code, and this trend seems to be unchanged to this day. Putting it another way, the Japanese IT industry still heavily relies on the 'waterfall' method, which places emphasis on planning and quality control before release. As a result, while the rate of bugs can be kept relatively low, it fails to keep up with rapid bursts of technological innovation, weakening competitiveness in the global market. In response to this situation, particularly in the field of cyber security, there are increasing calls for a shift in approach, away from competing by releasing innovative ideas or products to the international market, instead encouraging a focus on offering products and services that have fully integrated security features, in line with the concept of ‘security by design’. (Bartlett, 2018) Given Japan's attributes and strengths, this may rather be a sound rationale. However, in any case, in order to improve Japan's technological productivity in the cyber industry, it would be necessary to make a decision to move out of the rigid cultural and social conventions.

Specifically speaking, the IISS report mentioned the severe digital divide between the younger and older generations as a major cause of lagging behind in terms of Japan’s technological productivity by citing Organisation for Economic Cooperation and Development (OECD) suggestions. The OECD even indicated that Japan needs to increase investment in skills and digital capabilities, especially for middle-aged and older workers, in order to close the technological productivity gap with other OECD member countries (OECD, 2019). Japan still has a strong seniority-based system, and many top decision-makers, particularly many of the politicians and senior officials in government agencies who hold influential power over national initiatives, are unfortunately dominated by an analogue generation of IT technophobes - the elderly (Work Life Balance Co., Ltd., 2021). In other words, the social structure has not been updated enough, in which older generations who lack basic IT literacy are allowed to continue in positions of power without improving them.

b) **Information Dominance**: Japan’s pursuit of information dominance in cyberspace faces significant challenges rooted in constitutional, industrial, and educational limitations. These issues collectively impede the nation’s ability to secure and control critical information infrastructure, preempt cyber threats, and foster domestic innovation in cybersecurity. A major constitutional obstacle is Article 21(2). This legal framework restricts proactive data monitoring and intelligence-gathering activities, limiting Japan's capacity for large-scale surveillance and cyber espionage—essential elements for preempting and mitigating cyber threats. Such constraints create a structural disadvantage compared to nations with more flexible legal environments for cybersecurity operations. Compounding this challenge is Japan's limited accumulation of cybersecurity data and its dependence on foreign technologies.

According to Inoue, Japan has long viewed cybersecurity as a necessary but non-revenue-generating expense, unlike other advanced IT nations that integrate cybersecurity as a core component of their technological strategies. This perception has led to a market in which domestic security products account for less than 10% of all offerings, with reliance on foreign technologies remaining the norm. The lack of homegrown, market-competitive cybersecurity technologies creates a negative feedback loop: limited development leads to insufficient data accumulation, which in turn hampers innovation and further erodes Japan's capacity to achieve technological superiority in cybersecurity. Furthermore, the absence of a robust industry-government-academia ecosystem exacerbates these challenges. (Inoue, n.d.) While the need for collaboration between these sectors is widely recognized, Japan lacks sufficient infrastructure to support comprehensive cybersecurity education and research. For example, there are currently no educational institutions offering degree programs specifically dedicated to cybersecurity or cyber defence. The National Defence Academy (NDA) is preparing to launch a specialized course, but enrollment is not expected until 2028 (Nikkei Newspaper, 2023).

5. Technological Innovation and Human Capital

a) **Cyber Workforce Development**: One of the biggest challenges for both the private and public sectors is fostering and securing long-term employment for professional personnel. The supply-demand gap for cybersecurity personnel in Japan is estimated at around 110,000 (Oguma, 2024). The first step would be to develop attractive treatment and career paths for qualified and skilled personnel. In particular, public organizations including the CDU of the JSDF are severely lacking in terms of flexible career paths and role models that can attract talented and highly motivated people. For example, as information security expert Fumiaki Yamazaki points out, the current situation is that cyber JSDF personnel and cyber police officers are leaving the organization one after another after acquiring advanced qualifications. Unfortunately, with the conventional system of promotion, where salary and position are linked, there is no clear precedent or outlook for the career path of chief engineers or technicians in the field of cyber security. (Yamazaki, 2023)

Furthermore, the lack of notable, charismatic, and attractive personnel, in other words, role models, has exacerbated engineers' psychological hesitance towards becoming a public servant which requires them to have the low degree of self-discretion and selfless devotion (Nakatani, 2024; NISC, 2020). In order to reform the way organizations' ligid structure, it would be extremely valuable to foster individuals who can serve as commanders with persuasive leadership based on hands-on experience, provide flexible career paths that match the aspirations of human resources with the skills and abilities they possess, and create a system that ensures the mobility of human resources.

Finally, to address the human resource shortage in the JSDF's CDU, optimizing the reserve JSDF assistant system should be prioritized. Introduced in 1997 to bolster emergency preparedness within constitutional constraints, the reserve system comprises three components: 1) the rapid-reaction reserve component, 2) the main reserve component, and 3) the reserve assistant component. Of these, 3) the reserve assistant is intended for civilians who have never served in the JSDF, recruitment of cyber sector personnel was started in 2022. (The Cabinet Office of Japan, 2024) Given that the establishment of the CDU itself is still new, and the cyber and information processing field recruitment for the reserve Component is also relatively new, it can be said that the reserve JSDF related to cyber defence is still in its developmental stages. In fact, in a survey conducted in 2020 of 19 members of EDL CDU and 12 reserve JSDF who had been recruited for their information processing skills, the number of the reserve JSDF who were anxious before the start of their term was more than 10 times higher than in Estonia as shown is figure 4. Not only that, their level of satisfaction at the end of their term was also significantly lower than in Estonia as shown in figure 5. (Hidaka and Ide, 2020)

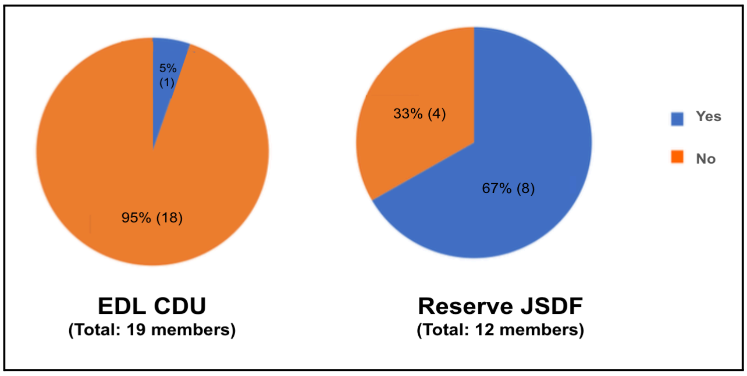

Figure 4. Prior Anxiety for Application (Source: Hidaka and Ide, 2020)

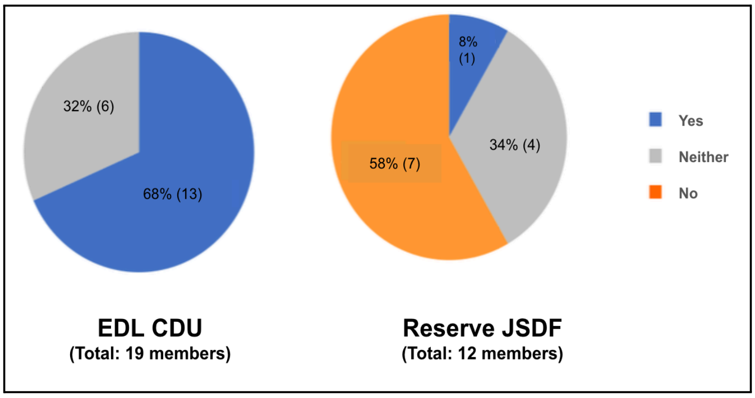

Figure 5. Satisfaction after Enlistment (Source: Hidaka and Ide, 2020)

Transforming the culture and image of the organization will require sustained efforts to cultivate "soft power," both internally and publicly. Such efforts would help attract skilled cybersecurity professionals and inspire them to contribute effectively to national security.

b) **Investment in Cybersecurity R&D**: As mentioned above, the cybersecurity industry was also unable to escape the effects of economic stagnation. This economic stagnation has accelerated the Japanese software development method of avoiding bugs and risks rather than quickly bringing innovative ideas to the world market. Although the Japanese economy and people's lives are heavily dependent on IT, domestic security products account for less than 10% of the total security products market. (Inoue, n.d.) In Japan, where there were already many large internet and telecommunications companies, such as NTT, KDDI (Kokusai Denshin Denwa International), Fujitsu and Rakuten, it is not so surprising that they preferred to introduce foreign security technologies that had already been proven rather than spend time and money developing domestic security products (Bartlett, 2018). Moreover, to date, Japan has been fortunate not to have experienced a massive and nationwide cyber attack that has brought its financial and telecommunications systems to a temporary and complete shutdown. Due to this background, a sense of crisis has been lacking, and the perception that cyber security is a necessary evil and a cost that does not generate revenue has taken hold for a relatively long time compared to other developed IT countries.

However, it should be noted that this good fortune is due less to the fact that Japan's cyber security is very advanced, and more to the fact that it has been spared intensive attacks due to the unique language barrier of Japanese. (Osawa et al., 2021) In fact, around 10 years ago, Japan was rarely targeted by cyber attacks and was considered a country with a low rate of malware detection. This good fortune started to fade away around 2016, when the era of “statistical translation” gave way to the era of “neural translation,” which uses systems modeled on the human brain. Google's machine translation system, which produced more natural and accurate translation results than statistical translation, surprised many people, and the distribution of this tool led to a significant increase in cyber attacks targeting Japan. (Crimson Japan, 2020: Security News, 2021) If Japan ignores or fails to correct this over-reliance on foreign products and intelligence, it will lead to a situation where core cyber defence and cyber security technologies are not cultivated and data resources are not accumulated domestically. Ultimately, this would create a negative spiral that would further hinder the growth of Japan's competitive edge in the cyber market. (Inoue, n.d.)

5.2 Estonia

1. Cyber Defensive Capabilities

a) **Cybersecurity Infrastructure**: Estonia's defence capabilities are rooted in a sophisticated, multi-layered cybersecurity ecosystem. The "Kyberturvalisuse Strateegia 2022" continues to evolve, with a draft update forthcoming (Riigi Infosüsteemi Amet (RIA), 2022). Additionally, Estonia's Critical Information Infrastructure Protection (CIIP) and the Estonian Computer Emergency Response Team (CERT-EE) ensure proactive defence of the country's information systems. CERT-EE, which operates under the RIA, is crucial for rapid incident response, coordination, and information-sharing across critical service providers. A cornerstone of Estonia's cybersecurity infrastructure is X-Road, a decentralized data exchange layer that securely facilitates data sharing across institutions without relying on centralized servers. This system employs encryption and strict access controls, significantly reducing the risk of data breaches. Furthermore, all data modifications and access are logged for auditing, enhancing both security and transparency. (Hardy, 2024) The foundation of these efforts lies in Estonia's strict data minimization principles, ensuring that only essential data is collected and used during intelligence operations. This reduces the risks associated with the handling of sensitive information as well. (DLA Piper , 2024)

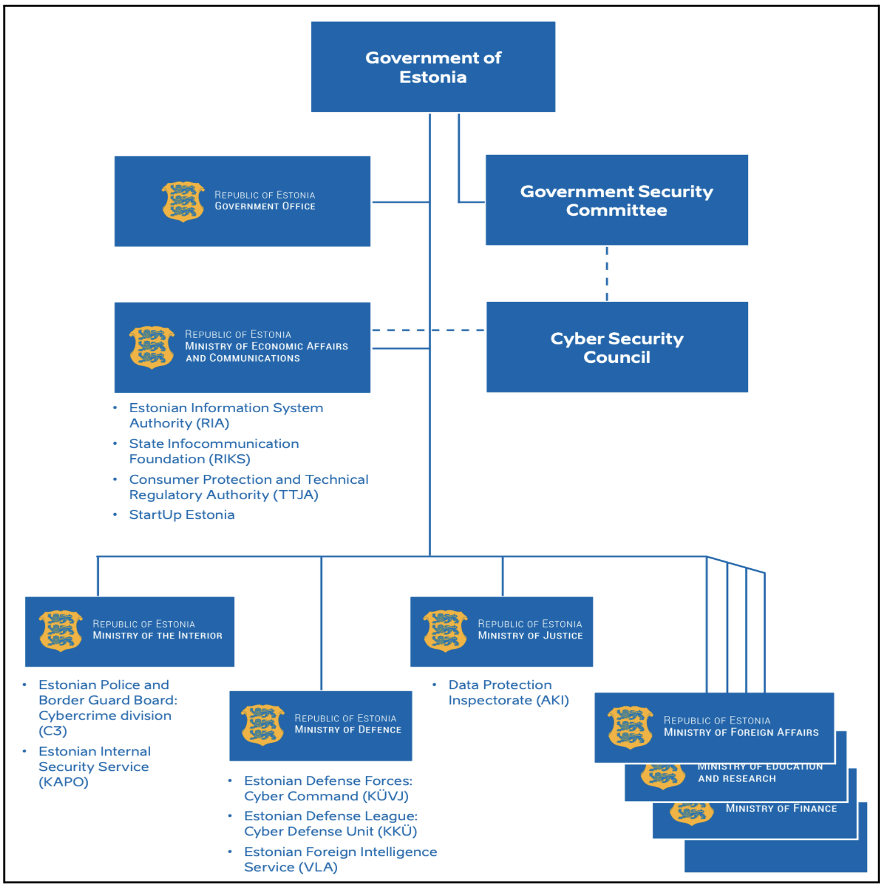
Government of Estonia
Republic of Estonia Government Office
Government Security Committee
Republic of Estonia Ministry of Economic Affairs and Communications
Cyber Security Council
Estonian Information System Authority (RIA)
State Infocommunication Foundation (RIKS)
Consumer Protection and Technical Regulatory Authority (TTJA)
StartUp Estonia
Republic of Estonia Ministry of the Interior
Estonian Police and Border Guard Board: Cybercrime division (C3)
Estonian Internal Security Service (KAPO)
Republic of Estonia Ministry of Defence
Estonian Defense Forces: Cyber Command (KÜVJ)
Estonian Defense League: Cyber Defense Unit (KKÜ)
Estonian Foreign Intelligence Service (VLA)
Republic of Estonia Ministry of Justice
Data Protection Inspectorate (AKI)
Republic of Estonia Ministry of Foreign Affairs
Ministry of Education and Research
Ministry of Finance

Figure 6. Cyber security governance in Estonia (RIA, 2020)

b) **Incident Response and Recovery**: RIA oversees the protection of the country's information and communications infrastructure, ensuring the security of vital service systems. The CIIP handles risk evaluations, data management on Critical Information Infrastructure (CII), sectoral coordination, information exchange, cybersecurity awareness, and national emergency response planning for large-scale cyber incidents. CERT-EE functions as an information-sharing system, managing incident handling, issuing alerts, and supporting relevant organizations. Critical service providers notify CERT-EE during security incidents, enabling timely reporting, efficient analysis, and swift response. (Yamaguchi, 2019) The Estonian military plays a critical role in national cyber defence, particularly during large-scale cyberattacks or hybrid threats. The Estonian Defence Forces and the Cyber Command collaborate with civilian agencies to provide additional resources, technical expertise, and operational capabilities. Their responsibilities include ensuring the continuous operation of IT services, as well as conducting both defensive and offensive cyberwarfare operations when necessary. This military involvement is crucial for strengthening the resilience of critical infrastructure and enabling effective recovery from sophisticated or state-sponsored cyber threats, exemplifying a well-integrated approach that combines military and civilian capabilities in Estonia's national cybersecurity framework. (Pau, 2018)

2. Cyber Offensive Capabilities

a) **Cyber Attack Capabilities**: While Estonia does not publicly emphasize its offensive cyber strategies, its involvement in the NATO CCDCOE, headquartered in Tallinn, reflects its commitment to enhancing both defensive and offensive capabilities within an international framework. Estonia’s leadership participation in NATO-led exercises, such as “Locked Shields”, underscores its readiness to conduct simulated cyber attacks for strategic defence purposes. These exercises not only test Estonia’s technical skills but also prepare it for real-world scenarios where offensive measures may be required to deter or respond to cyber threats effectively. These offensive capabilities and intelligence strategies collectively position Estonia as a leader in leveraging cyber power to protect its sovereignty and contribute to global cybersecurity initiatives. (CCDCOE, 2023)

b) **Cyber Intelligence and Espionage**: Estonia has established robust cyber intelligence and espionage mechanisms, largely driven by its experience with the 2007 cyberattacks attributed to Russia. These attacks served as a catalyst for developing sophisticated cyber intelligence capabilities. Estonia employs advanced monitoring tools and collaborates with international partners, including NATO and the EU, to gather intelligence on cyber threats. The RIA, Estonia’s Information System Authority, plays a central role in coordinating intelligence efforts related to cybersecurity. By integrating intelligence sharing with its allies and investing in advanced data analytics, Estonia ensures proactive threat detection and enhances its ability to anticipate and counter cyber threats. Moreover, Estonia’s emphasis on building a digitally literate population and fostering expertise in areas like intrusion detection, cryptography, and blockchain further strengthens its cyber intelligence ecosystem. (RIA, 2020)

3. Legal and Policy Frameworks

a) **National Cybersecurity Policies**: Estonia has a Cybersecurity Act, which clearly defines the responsibilities of critical service providers, such as risk analysis and business continuity planning, measures to prevent interruption of critical services, and notification in case of emergency, and imposes certain obligations on critical service providers to ensure cyber security. (Parliament of Estonia, 2018) In 2009, the “Cyber Security Council” was added to the Estonian Government Security Committee to promote strategic inter-ministerial cooperation and to oversee the achievement of the goals of the cyber security strategy. In 2011, the responsibility for cybersecurity policy formulation, which had previously been handled by the Ministry of Defence, was transferred to the Ministry of Economy and Communication, and the RIA was established as the entity to implement cybersecurity policy in Estonia. (IISS, 2023) Additionally, Estonia fully aligns with the EU's General Data Protection Regulation (GDPR), ensuring strong data protection and compliance with European privacy standards (DLA Piper, 2024). This alignment underscores Estonia's commitment to robust legal frameworks that integrate national cybersecurity policies with international regulations.

b) **International Cooperation**: Estonia has been highly trusted by the EU in cybersecurity technologies and solid IT infrastructure. In 2008, the country succeeded in inviting the CCDCOE, an operationally independent international military organisation, to its capital, Tallinn. Although the CCDCOE is not responsible for NATO’s cyber security, its publications, such as the Tallinn Manual; an annual conference, such as CyCon (Cyber Conflict); and training exercises, such as Locked Shields, do have a significant influence on the growing cyber capability of NATO. However, despite its accomplishments, Estonia is not immune to challenges. An audit by the National Audit Office of Estonia highlighted critical shortcomings in the safety and preservation of its databases. The report identified “significant deficiencies” in information security and the absence of a comprehensive legal framework, exposing vulnerabilities within Estonia's e-government ecosystem. These findings underscored the need for more robust measures to protect the country's digital assets. (Mattson, 2018) In response, Estonia adopted an innovative approach to address these challenges by dispersing risks across borders. One notable initiative is the “Data Embassy” partnership with Luxembourg, the first of its kind globally. Through this collaboration, Estonia stores critical government data in Luxembourg's secure data centres. This arrangement ensures digital continuity and resilience, even under extreme scenarios, such as cyberattacks, natural disasters, or territorial loss. By leveraging Luxembourg's advanced infrastructure and legal protections, Estonia mitigates the risks associated with its domestic vulnerabilities. As stated in the article “The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis”, this initiative also carries risks. For example, there are certain risks involved in storing and maintaining data in remote locations across borders, and the potential threat of man-made or natural disasters is also not zero. In addition, the lack of sufficient legal precedents could also raise concerns. However, the Estonian government decided to enter into this bilateral agreement after weighing up the potential loss of the social trust in e-government that it worked so hard to build over the past 15 years. (Robinson, Kask and Krimmer, 2019)

4. Economic and Political Influence through Cyber Capabilities

a) **Cyber-Related Economic Strength**: Estonia makes the most of its position as a hub for international cybersecurity cooperation, attracting many digital companies, research institutions and talent from inside and outside Europe. As well as physical migrants, Estonia has also welcomed more than 100,000 people from more than 170 countries as e-Recidents through the e-Residency programme, which was launched in 2014, and to date more than 27,000 businesses have been established by e-residents. (The Government of Estonia, 2023) The programme is making Estonia an attractive location for global entrepreneurs and companies and bolstering the vibrant and innovative start-up ecosystem that has created Skype, Wise and Bolt. Furthermore, as Estonia faces challenges such as a shortage of human resources as a small country and national security threats from neighbouring Russia, increasing the number of stakeholders and supporters around the world who engage with Estonia through the NATO/EU platform and progressive government initiatives, is a very meaningful and effective means to address the situation. In this way, the international support base will be reinforced and the sustainable development of the digital economy will be made possible. These efforts not only ensure the security of Estonia's digital infrastructure, but also attract foreign investment, promote innovation in the cyber sector and are an important contributor to Estonia's economic growth. (Kohler, 2020; Hankewitz, 2024)

b) **Information Dominance**: Estonia has leveraged its digital innovation and cybersecurity successes to become an influential voice in promoting cyber norms. Former President Toomas Hendrik Ilves was instrumental in this, positioning Estonia as a “cyber norm entrepreneur” within NATO and beyond. Through initiatives advocating for responsible cyber behaviour and legal norms, Estonia has become a prominent advocate for establishing rules and ethical standards in cyberspace. (Crandall and Allan, 2015)

5. Technological Innovation and Human Capital

a) **Cyber Workforce Development**: In 1996, five years after gaining independence from the Soviet Union, Estonia launched the “Tiger’s Leap” program, aiming to equip all schools with computers and connect all educational institutions to the Internet. (Kumagai, 2021) This foundational initiative laid the groundwork for Estonia's robust cyber workforce development. Programming classes are introduced at an early stage, and from secondary school, students have the opportunity to study internet security, cyber defence, and even hacking techniques through subjects like "National Defence." (Starthome, 2022) These early education initiatives ensure that students gain a strong foundation in IT and cybersecurity from a young age. In higher education, institutions such as Tallinn University of Technology (TalTech) and the University of Tartu offer advanced courses in cybersecurity. TalTech also houses the Centre for Digital Forensics and Cyber Security, which collaborates with government agencies and plays a pivotal role in strengthening Estonia's cyber resilience. This centre contributes to global advancements in cybersecurity knowledge and capabilities. (e-Estonia, 2022) As a result of these comprehensive educational initiatives, Estonia has cultivated a large pool of experts skilled in areas such as system design, cryptography, intrusion detection, and blockchain. (Invest in Estonia, n.d.) The practical application of these skills is facilitated through initiatives like the Cyber Command, which integrates cybersecurity training with national defence. This program allows IT students to fulfil mandatory military service while gaining hands-on experience in cybersecurity operations. (Põldma, 2021) Additionally, Estonia established the CDU of the EDL in 2011. This volunteer organization recruits and trains civilians to assist in cyber defence operations during crises, working in collaboration with the Estonian Defence Forces and other government agencies. (Kaska, Osula, and Stinissen, 2013) Estonia's commitment to providing citizens with early opportunities for IT and cybersecurity skills acquisition, combined with fostering a strong awareness of their role in national protection, reflects a whole-of-society approach to security. These efforts demonstrate how a nation can successfully mobilize its human resources to ensure robust cybersecurity and resilience.

b) **Investment in Cybersecurity R&D**: Leaders and security specialists from many countries, not only from the EU countries but also from Asia and Africa, visit Estonia, where active interactions and cooperation occur. The progressive domestic initiatives and international contributions have generated a favourable cycle, and now Estonia is called the hub of cyber defence. (Boeke, 2016) A number of Estonian domestic-origin startups and enterprises have also emerged since Estonia became a cybersecurity leader, such as Cybernetica and many others. (e-Estonia, 2017) Not only that, the world's leading cyber security companies, such as Symantec and Malwarebytes, also trust and choose Estonia as a base for R&D (Invest in Estonia, n.d.). Proactive initiatives, both domestically and internationally, have pushed Estonia to the point where it is now called a cyber defence, digital, and innovation hub.

5.3 South Korea

1. Cyber Defensive Capabilities

a) **Cybersecurity Infrastructure**: South Korea has earned a strong reputation as a leader in digital governance by adopting a highly centralized approach to its cybersecurity and digital governance frameworks. This centralized model enables rapid, efficient responses to daily cyber threats while optimizing resource use, particularly in managing limited personnel.

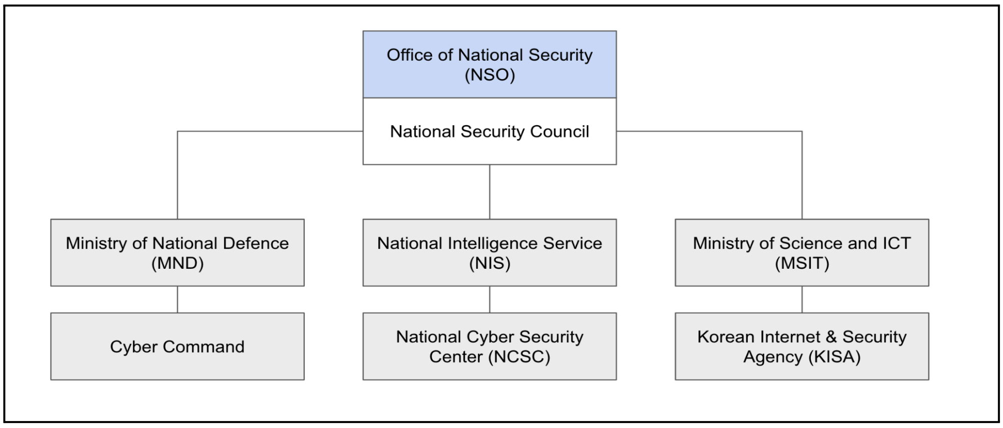
Office of National Security (NSO)
National Security Council
Ministry of National Defence (MND)
National Intelligence Service (NIS)
Ministry of Science and ICT (MSIT)
Cyber Command
National Cyber Security Center (NCSC)
Korean Internet & Security Agency (KISA)

Figure 7. Cyber defence Structure of South Korea

(Source: Korean Policies of Cybersecurity and Data Resilience)

The country's cybersecurity infrastructure is coordinated under the Office of National Security (NSO) and the National Security Council, which oversee strategic decision-making and coordination among key government agencies. This central structure includes:

- ○ The Ministry of National Defence, which operates the Cyber Command to address military cyber threats and strengthen national defence.
- ○ The National Intelligence Service (NIS), which hosts the National Cyber Security Center to manage and respond to threats against government and critical infrastructure systems.
- ○ The Ministry of Science and ICT(information and communications technology), which oversees the Korea Internet & Security Agency (KISA) and its Korea Internet Security Center (KISC).

(Kim and Bae, 2021)

b) **Incident Response and Recovery**: KISC, managed by KISA, plays a vital role in securing over 400 critical infrastructure systems, including approximately 150 systems operated by private-sector providers. This security program is funded by the government and offers five essential services:

1. 24/7 monitoring of critical infrastructure systems for threats.
2. Detection of vulnerabilities and cyber incidents.
3. Analysis of potential or ongoing cyber threats.
4. Response support to mitigate and recover from cyber incidents.
5. International collaboration.

If a website is attacked by a DDoS attack, critical infrastructure providers can rent a DDoS shelter provided by the government. (Uesugi, 2018) In addition, KISA started employing an automated threat information sharing system called the Cyber Threat Analysis System (C-TAS) in 2014 to share threat information with private companies and academic institutions. The C-TAS is free to join and involves government agencies, cybersecurity companies, internet shopping, online gaming, etc. Information provided by companies is processed anonymously by the government, and the results of the analysis are shared widely with participants, which helps to share information rapidly and improve their response to incidents. Since 2017, C-TAS has introduced big data analytics and machine learning, and evolved to offer a dashboard to visualise cyberattack typologies and threats information. (Cho.C, 2017) The government also provides extensive public support, including: Forced warning messages from Internet Service Providers with malware removal instructions, free malware removal software, and a one-stop cybersecurity helpline for public inquiries.

2. Cyber Offensive Capabilities

a) **Cyber Attack Capabilities**: South Korea's cybersecurity strategy emphasizes offensive capabilities to counter persistent North Korean cyber threats (Valeriano and Leasure, 2024). This aligns with the “Offensive Cyber Security Strategy” announced in September 2024, aimed at deterring future attacks and demonstrating a stronger cyber posture (Da-gyum, 2024). North Korea’s advanced hacking tactics, leveraging AI technologies like advanced persistent threats (APTs) and generative language models, focus on espionage and sabotage. To counter such threats with limited resources, South Korea integrates cutting-edge technologies like AI to identify sources, assess damage, and mitigate risks (Valeriano and Leasure, 2024). Another motivation for South Korea to develop its offensive capabilities is the imbalance inherent in North Korea's cyber capabilities - that is, the fact that the focus is on attacks in the cyber domain - means that the isolated regime is highly vulnerable to cyber attacks by hostile countries. It is said that the cost of defending against cyber attacks is higher than the cost of attacking, therefore, in light of economic sanctions and isolation from the international community, there is no contradiction. Given this background, rather than maintaining a purely defensive posture, the South Korean strategy of switching to a more aggressive stance should have overwhelmingly more advantages, despite the costs incurred and the negative impact on its own soft power. (Song, 2023)

Of course, the integration of AI into offensive cyber security strategies naturally entails ethical and privacy dilemmas. This is because the collection and analysis of a wide range of data is inevitably necessary, and there is a possibility that these will infringe on individual rights. (Eom, 2024) However, in the case of South Korea, the constant threat from North Korea has threatened the ultimate and greatest goal of "national survival", and the fact that there is no strong opposition among the people to prioritizing national security over privacy has further encouraged this transition (TBS NEWS DIG, 2024).

b) **Cyber Intelligence and Espionage**: Cyber Intelligence and Espionage: As highlighted in the National Cyber Security Strategy, the South Korea considers not only the integration of advanced state-of-the-art technology into cyber security, but also a collective defence framework and agreement based on active information sharing and close collaboration to be of great importance (Eom, 2024). Although the authority to investigate counter-espionage operations was transferred from the NIS to the National Police Agency with effect from 1 January 2024, the NIS plays a pivotal role in protecting South Korea against cyber threats, including those from state actors like North Korea and China. (Lee and Lee , 2024).

In 2022, the NIS became the first Asian member of the NATO CCDCOE, enhancing its capabilities through international collaboration. (Campbell, 2022) Moreover, the country initiated the "Strategic Cybersecurity Cooperation Framework" with the US in April 2023, decleared their shared commitment to countering cyber threats and exchanging vital intelligence. In December of the same year, it also announced its participation, together with the US and Japan, in trilateral talks on North Korea's cyber activities in December. (Eom, 2024) However, South Korea also has several issues to be addressed in coming years with regard to the delegation of authority for counter-espionage operations, such as the decline in specialisation and concerns about political neutrality (Lee and Lee , 2024).

3. Legal and Policy Frameworks

a) **National Cybersecurity Policies**: In 2024, the South Korean National Intelligence Service announced that the average number of cyber attacks on South Korea would reach 1.62 million per day by 2023, with 80% of these being carried out by North Korea. In response, the South Korean government announced a new national cyber security strategy that same year, focusing on strengthening its “preemptive” and “offensive” capabilities to counter the growing threat of cyber attacks from North Korea, as well as promoting international cooperation and the adoption of cutting-edge technology. (Kwak, 2024) South Korea had already begun to adopt an active defence approach that utilized AI technology to detect intrusions and narrow down targets (Park and Reddy, 2024), and in April 2024, they established the “Defence AI Center” which aimed to further research and advance technologies. The center is operated as part of the “National Defence Innovation 4.0” project launched by the South Korean government in March 2023, and it is focusing on strengthening South Korea's proactive defence capabilities through collaboration between industry, government, and academia (Kim, 2024). The government and citizens are strongly aware that the integration of AI into cybersecurity could be a major technological opportunity for South Korea, and they have high expectations (Eom, 2024). Through such efforts, South Korea has a clear vision of establishing a leading position in the formation of international norms by sharing their knowledge and technology with allied countries and contributing to the stabilization of the international community (Valeriano and Leasure, 2024).

b) **International Cooperation**: South Korea employs a dynamic approach to international cooperation as part of its soft power strategy in diplomacy, focusing on IT and cybersecurity collaboration (Kim, 2022). As already mentioned, it has strong working relationships with the US, NATO and Japan, while also placing a high value on supporting developing countries through establishing global research and education institutions. For example, the Global Cybersecurity Centre for Development (GCCD) was established in 2015. The objective of the GCCD is to support practical knowledge sharing and capacity building in the field of cybersecurity, and primarily offers a series of programmes aimed at public sector policymakers and professionals in developing countries. (KISA, 2021) By sharing its expertise and resources with developing countries, South Korea has the opportunity to strengthen its geopolitical position and lay solid foundations for broader and credible partnerships. Ultimately, these initiatives seek to contribute to the reinforcement and stabilisation of international norms in cyberspace. (Eom, 2024)

4. Economic and Political Influence through Cyber Capabilities

a) **Cyber-Related Economic Strength**: The country's technological development journey, often dubbed the "Miracle on the Han River", began in the aftermath of the Korean War. With a strong emphasis on education, innovation, and government support, South Korea strategically invested in its technological infrastructure, leading to remarkable progress (Shiy, 2020). South Korea is in third place after Denmark in first place and Australia in second place, regarded as one of the best digital governments in the world (MIC, 2023). In 2017, "Government 24", a one-stop portal that enables citizens to complete various administrative procedures for daily life online, was launched in full-scale service (Cho.S, 2022). As for the most significant feature of the e-government of South Korea, including the above, all of which are highly evaluated by the citizens, the usage rate is 87.6%, the recognition rate is 93.8%, and the satisfaction rate is 97.8%. (Nomura, 2020) The series of successes in digital government projects has led to great trust from the citizens in the government's technological capability.

b) **Information Dominance**: Cyber-attacks from North Korea are no longer just threats to South Korea but worldwide. North Korea exploits the asymmetry between the attacker and the defender in cyberspace to cover the disadvantages caused by economic sanctions and isolation from the international community, as well as to fulfil its objective of inflicting damage against hostile states. This asymmetry between attacker and defender involves both costs and risks. Attackers have many ways to make it difficult for defenders to trace them, such as multiple virtual private network and other means to evade tracking, or the use of numerous anonymous tools. In contrast, it is still not straightforward for defenders to pinpoint the exact source of an attack when it occurs. To mitigate this imbalance, South Korea has taken countermeasures by leveraging its status as North Korea's number one target, analysing its attack patterns, tools and intentions, and then sharing these widely with allies and collaborating countries, as well as accusing North Korean's wrongdoings with evidence to the international community. (Kshetri, 2014)

5. Technological Innovation and Human Capital

a) **Cyber Workforce Development**: In 2022, South Korea launched the 100,000 Cyber Security Personnel Training Plan, aiming to train a skilled cyber workforce by 2026. This plan, coordinated across multiple government ministries, focuses on developing 60,000 cybersecurity professionals and 40,000 supplementary personnel, and includes initiatives like white-hat hacking programs. As a result, KISA revealed that as of 2023, a total of 19,000 human resources have already been trained. This workforce expansion is critical for supporting South Korea's cyber defence and forms part of the strategy to launch a Cyber Reserve Force by 2025. (AFPBB News, 2023) Furthermore, in higher education institutions, the number of specialised research and teaching programmes to train high-level professionals and white hackers is increasing rapidly every year, with various programmes and scholarships available. For example, joint programmes with security companies offer 100% scholarships on condition of a guaranteed job after graduation, while Korea University's CYDF, established in 2012, is a joint programme with the South Korean Army that offers security education with scholarships on condition that students are commissioned for seven years after graduation. The CYDF is modelled on the Israeli Talpiot programme, where only the top 1% of students with the highest grades are eligible for the programme. These initiatives have been successful, with the Korean team achieving first place at DEFCON (Defence Readiness Condition) Capture the Flag 23 in the US and excellent results in other international hacking competitions. (Kim, 2015)

b) **Investment in Cybersecurity R&D**: South Korea's Digital Strategy of Korea, published in 2022, aims to position the nation as a global leader in digital innovation by 2027, with cybersecurity identified as one of six priority areas alongside AI, AI semiconductors, 5G/6G, quantum technology, and the metaverse. Recognizing cybersecurity as a cornerstone of its digital goals, South Korea is advancing research in areas like AI-driven threat detection, blockchain-based data security, and post-quantum cryptography. (Kan, 2022) To realize these goals, South Korea has committed to building a robust cybersecurity ecosystem through:

   ○ Significant R&D Investments: The government plans to invest over 1 trillion won to expand the size of the information protection market from 16 trillion won in 2022 to 30 trillion won by 2027.

   ○ Industry-Government-Academia Collaboration: Coordinated efforts to foster innovation, advance R&D capabilities, and translate breakthroughs into scalable solutions.

   ○ Cyber Workforce Development: Training a new generation of cybersecurity professionals to meet the demands of a rapidly evolving digital landscape.

(AFPBB News, 2023)

VI. Findings & Strategic Recommendations

6.1 Evaluating Japan's Cyber Defence Lag: Findings and Causes

While Japan is often ranked behind global cyber leaders in various indices, concluding that its cyber defence is unequivocally underperforming oversimplifies the issue. Japan’s unique constitutional and economic constraints, cultural values, and historical context all contribute to its current positioning, offering a nuanced perspective on its cyber defence posture.

1. **Constitutional and Legal Constraints**: Japan’s Article 9 of the Constitution, which renounces war, limits its ability to develop offensive ACD capabilities. Coupled with Article 21(2), which guarantees the secrecy of communications, these restrictions hamper proactive cyber intelligence and real-time threat mitigation. These legal provisions contrast sharply with countries operating without such constraints, putting Japan at a structural disadvantage in global rankings.
2. **Cultural and Identity Considerations**: Japan's pacifist identity and emphasis on peace and democracy are deeply rooted in its societal values. These factors limit public support for aggressive cyber defence measures, which are often perceived as incompatible with Japan's diplomatic ethos and post-war reconciliation efforts. Abrupt shifts in policy could jeopardize public trust and strain Japan’s relationships with neighbouring countries, particularly those with historical grievances. Additionally, Japan’s economic stagnation over recent decades and its traditionally conservative approach to governance have impacted its investment in innovation and cybersecurity R&D. Decision-making in these areas often prioritizes minimizing risks over pursuing bold, innovative ideas.
3. **Geopolitical and Strategic Priorities**: Japan’s prioritization of soft power diplomacy and restrained military strategies reflects a calculated balance. Unlike nations that emphasize hard power in cyberspace, Japan leverages its

technological expertise and cultural influence to foster global trust and cooperation, a strategy less suited for aggressive ACD initiatives. Furthermore, Japan's soft power in diplomacy is heavily weighted towards cultural assets and has little affinity with cyber power or national security.

4. **Lack of sense of urgency and advocacy to global society:** There is a significant lack of urgency in the public debate on cyber threats and defence strategies in Japan. This is simply due to the fact that there is not always a country with a level of hostility or tension that endangers national survival, and that the country has been spared from serious cyber damage, such as the partial shutdown of the national digital infrastructure due to language barriers. Japan's long-standing security relationship with the US would also have accelerated a sense of security that Japan is safe. On the other hand, despite this background, Japan has also produced a number of achievements that deserve international recognition. Examples include the success of the Tokyo 2020 Olympic without delay despite the fierce cyber-attacks, which were said to be the most numerous in history, and the establishment of a joint monitoring system for the formation of a cyber-security community in the Asian region. However, these achievements and initiatives have not been actively promoted to international society through globally influential media.

Although some constraints and inefficiencies exist in Japan's cyber defence, it is more accurate to attribute these to structural and legal limitations rather than negligence or oversight. Japan's constitutional constraints, particularly its commitment to pacifism under Article 9 and legal safeguards such as Article 21, have hindered its ability to transition to ACD measures. This real-time monitoring and response capability is a critical factor in global cybersecurity rankings. Japan’s delay in adopting such measures places it at a disadvantage compared to countries with fewer legal and ethical constraints. While Japan must remain flexible and prepare for potential shifts in policy—such as constitutional amendments or redefined strategies—it is crucial to recognize the cultural and ethical underpinnings of Japan's identity as a peace-oriented nation. Even if Japan adopts a more proactive cyber defence posture, its approach to offensive cyber capabilities and intelligence operations is likely to remain strategically and ethically restrained. Maintaining minimal reliance on aggressive tactics aligns with Japan's national values and could serve as a diplomatic advantage internationally, where neutrality and ethical standards are increasingly valued.

By leveraging this identity, Japan can be a trusted and diplomatically valuable partner in global cybersecurity. Balancing advancements in cyber defence with its commitment to peace and ethics could transform perceived limitations into strengths, fostering international collaboration and reinforcing its cultural integrity on the global stage.

6.2 Insights for Japan: Learnings from Estonia & South Korea

Japan faces unique challenges and opportunities in developing a robust cyber defence strategy. Instead of mirroring the strategies of established cyber powers, Japan should focus on creating a bespoke cyber defence approach that aligns with its values, strengthens its soft power, and effectively addresses its specific challenges. Drawing insights from Estonia and South Korea, Japan can take measured steps to define its role in the international cybersecurity landscape and utilize its cyber power to achieve national and global objectives.

1. Establishing a Clear Vision for Cyber Power and Advancing ACD Discussions with Public Trust

Both Estonia and South Korea showcase the necessity of a well-defined vision for cyber power as a cornerstone of their national security and diplomatic strategies. Estonia, faced with persistent cyber threats from Russia, has used cybersecurity to fortify its defence and international influence. Similarly, South Korea, under constant pressure from North Korea, has integrated cybersecurity into its strategic defence framework and regional diplomacy. For Japan, clarifying its desired position in the international community and defining the role of cyber power in achieving that vision are imperative. Japan must consider how cybersecurity can not only enhance national defence but also support peaceful, disciplined contributions to the global order, in alignment with its constitutional principles. Furthermore, the adoption of ACD must be approached transparently, with an emphasis on public trust. South Korea’s integrated government-public and step-by-step approach, and Estonia’s robust privacy frameworks provide valuable lessons on fostering trust and addressing public concerns. Japan should ensure that ACD discussions are aligned with constitutional values, prioritize privacy, and emphasize mutual benefits for national security and citizens.

Recommendations for Japan:

- **Define a Comprehensive Vision for Cyber Power**: Develop a clear, strategic vision for leveraging cybersecurity as a national asset. Firstly, defining its position in the international community and clarifying the role it seeks to play is critical. Japan must ask: What influence does it want to exert, and how can cyber power support this. By framing cybersecurity within a broader vision of peaceful and disciplined international contribution, Japan can align its cyber strategies with its constitutional values and its historical emphasis on diplomacy.
- **Foster Transparent ACD Discussions:** Promote open and inclusive discussions about ACD measures, ensuring alignment with democratic values and public concerns. These discussions should highlight how ACD can complement Japan's pacifist stance while improving national resilience against cyber threats.
- **Build Public Trust Through Citizen-Centric Benefits:** Demonstrate how cybersecurity advancements, including ACD, benefit citizens by protecting critical infrastructure and digital services. Emphasize strong privacy protections and ensure that the public sees tangible, reciprocal advantages from Japan’s cyber strategies.

2. Promoting Cybersecurity Talent Development and Ecosystem Building

Both Estonia and South Korea maintain strong and stable human resource pipelines, supported by compulsory military service and robust collaboration between industry, government, and academia. Estonia has raised IT literacy and cybersecurity awareness through early education initiatives like the 'Tiger's Leap' program, integrating programming and cybersecurity education from primary school onward. Higher education institutions offer advanced training, while the military, CDU, and EU/NATO cybersecurity R&D organizations provide practical application opportunities. Additionally, private companies and start-ups contribute to Estonia's digital government. South Korea focuses on the ‘100,000 Cyber Security Human Resources Development Plan,’ fostering skilled professionals through higher education and regional programs. The government collaborates with the private sector, particularly ICT companies and start-ups, to provide career pathways for trained personnel. Both countries have built sustainable human resource ecosystems, offering valuable models for Japan’s future cybersecurity workforce development.

Recommendation for Japan:

- **Establish Dedicated Cybersecurity Education Programs:** Japan should prioritize the creation of dedicated cybersecurity degree programs and courses in universities and higher education institutions, including the NDA. This would provide a formal pathway for developing high-skilled cybersecurity professionals, starting from foundational IT and cybersecurity education at early stages to advanced specialized training at the tertiary level.
- **Foster Industry-Government-Academia Collaboration:** To build a sustainable talent pipeline, Japan needs to strengthen partnerships between the government, private sector, and educational institutions. For example, the private sector can assist students studying specialised cybersecurity skills with job placement commitments, or provide internship opportunities with the JSDF CDU or other governmental agencies. It would also be important to lower the

barriers between the private and public sectors and increase the mobility of human resources.

- **Enhance Participation and Engagement in Cyber Reserves:** Revamp the cyber reserve system to improve participant satisfaction and engagement by addressing fears about involvement, providing clear tasks and offering practical, rewarding experiences.

3. Strengthening International Communication and Advocacy through Cyber Power

Both Estonia and South Korea actively leverage their cybersecurity achievements as tools of soft power to enhance their international influence. Estonia has positioned itself as a global cybersecurity leader by sharing its technologies, expertise, and experiences with NATO, the EU, and other partners, showcasing its resilience and innovation. South Korea regularly participates in high-profile regional collaborations and global cybersecurity forums, emphasizing its commitment to a secure digital environment. For Japan, linking its cyber power to diplomatic soft power is essential. While Japan has a reputation for cultural diplomacy, it has yet to fully capitalize on its potential in cybersecurity as a tool for global influence. By aligning its cybersecurity strategies with its broader diplomatic objectives, Japan can strengthen its global presence and foster international trust and cooperation.

Recommendations for Japan:

- **Integrate Cyber Power with Diplomatic Messaging:** Clearly articulate how Japan’s cyber power supports global peace, security, and prosperity. Highlight achievements in both soft power areas and hard power results. Position these efforts as contributions to a disciplined and peaceful global society.
- **Enhance International Visibility:** Publish research findings, cybersecurity initiatives, and innovative practices in English and other widely spoken

languages to reach a broader audience. Leverage global media platforms, international conferences, and academic publications to share Japan's vision for cyberspace and demonstrate leadership in cybersecurity.

- **Collaborate and Advocate Through Global Platforms:** While it is important to embrace innovation and bold thinking, Japan should prioritise utilising the strengths it possesses too, such as 'security by design' and expertise in disaster management, and gradually increase its international recognition and credibility. It is also true that Japan could offer a new and unique perspectives to the international community by steadily promoting those ideas and efforts on a global platform.

4. Modernizing Practices in Public Institutions

Japan's autonomous private sector approach to cybersecurity reflects its population size and advanced private IT industry but would benefit from stronger government-academia collaboration. Estonia's e-Estonia initiative highlights the value of collaborative frameworks, integrating digital ID (Identity document), e-governance, and infrastructure protection. South Korea's KISA showcases the effectiveness of government-driven partnerships in advancing targeted cybersecurity research like AI-driven threat detection and blockchain security.

Recommendations for Japan:

- **Adopt Flexible Career Pathways and Remuneration Systems:** Japan should introduce flexible career pathways and performance-based reward systems to attract and retain top-tier talent in cybersecurity. Learning from private sector practices, government institutions can offer competitive salaries and career growth opportunities that align with modern employment trends.
- **Focus on Merit-Based Leadership and Commander-Level Training:** Moving away from traditional seniority-based promotions, Japan should prioritize merit-based leadership appointments, ensuring leaders possess both technical

expertise and proven operational experience. Implementing commander-level training programs can prepare leaders to act decisively during cyber crises, ensuring effective top-down coordination in emergencies.

- **Promote Practical and Collaborative R&D Efforts:** Japan should encourage collaborative R&D efforts that integrate government, private sector, and academia and focus on fostering innovation in promising areas such as AI-driven threat detection and quantum encryption. Additionally, establishing international joint innovation hubs or research centers that bring together diverse stakeholders can accelerate the development of cybersecurity technologies.

VII. Conclusion

This thesis set out to evaluate Japan’s cyber defence capabilities through the lens of Cyber Power Theory and to explore whether Japan's lagging position is a result of structural deficiencies or strategic choices. It also sought to identify lessons Japan can learn from Estonia and South Korea to improve its cyber power and strategic positioning. The findings reveal that Japan’s perceived lag in cyber defence stems not solely from technical inadequacies but also from systemic challenges, including fragmented organizational structures, limited real-time monitoring due to constitutional constraints, and insufficient investment in cybersecurity R&D. Despite these challenges, Japan has demonstrated unique strengths, such as its ability to prevent disruptions during high-profile events like the Tokyo Olympics and its strategic use of backups to reduce ransomware vulnerability. These reflect Japan’s meticulous and risk-averse approach, which aligns with its broader cultural and constitutional values.

Lessons from Estonia and South Korea highlight the importance of fostering collaboration between government, private sector, and academia. Estonia’s integration of public-private partnerships through initiatives like e-Estonia and South Korea’s proactive government-led training programs and AI-driven innovations underscore the value of leveraging collective expertise to address modern cyber threats. These models emphasize the need for Japan to adopt a more collaborative and flexible framework while retaining its distinct cultural and ethical approach.

Ultimately, Japan’s path to strengthening its cyber power lies in balancing its constitutional constraints with modern security needs. By prioritizing structured public-private collaboration, investing in cybersecurity R&D, and fostering globally competitive talent, Japan can carve out a unique role in the international cyber landscape—one that harmonizes its pacifist identity with proactive and ethical cyber defence strategies. This approach will enable Japan to not only improve its national security but also to contribute to shaping global norms in cyberspace.

List of References

AFPBB News (2023). 韓国政府、情報セキュリティ市場に*1000*億円投資*...2027*年には*3*兆円規模に拡大. [online] Afpbb.com. Available at: https://www.afpbb.com/articles/-/3482015 [Accessed 8 Dec. 2024].

Akaha, T. (2005). *'Soft Power' in Japan's Security Policy: Implications for Alliance with the US. Pacific Focus*, 20(1), pp.59–91. doi:https://doi.org/10.1111/j.1976-5118.2005.tb00309.x.

Asia Society (2023). *Cartan McLaughlin: High Risk Japan — How Vulnerable is Japan to Cyber Attacks?* [online] www.youtube.com. Available at: https://www.youtube.com/watch?v=PFmvU08KNSs [Accessed 10 May 2024].

Bartlett, B. (2018). *Government as facilitator: how Japan is building its cybersecurity market.* Journal of Cyber Policy, 3(3), pp.327–343. doi:https://doi.org/10.1080/23738871.2018.1550522.

Bennett, A. (2004). *Case Study Methods: Design, Use, and Comparative Advantages.* In D. F. Sprinz, & Y. Wolinsky-Nahmias (Eds.), Models, Numbers, and Cases: Methods for Studying International Relations (pp. 19-55). Ann Arbor: The University of Michigan Press.

Bendiek, A. and Bund, J. (2023). *Shifting Paradigms in Europe's Approach to Cyber Defence: Ambitions to Disrupt Malicious Cyber Activity Need to Protect Norms as Well as Networks.* SWP Comment, [online] 48. doi:https://doi.org/10.18449/2023C48.

Campbell, C. (2022). *South Korea's Spy Agency Joins NATO's Cyber Defence Unit.* [online] Time. Available at: https://time.com/6173812/south-korea-cyber-nato-china/ [Accessed 9 May 2022].

CCDCOE (2023). *World's largest cyber defence exercise Locked Shields kicks off in Tallinn.* [online] Ccdcoe.org. Available at: https://ccdcoe.org/news/2023/worlds-largest-cyber-defense-exercise-locked-shields-kicks-off-in-tallinn/ [Accessed 15 Dec. 2024].

Cho, C. (2017). サイバーセキュリティコミュニケーションに関する日韓比較研究 ○趙 章恩(東京大学) A comparative study between Japan and Korea on cyber security communication. 横幹連合コンファレンス予稿集, [online] 8. doi:https://doi.org/10.11487/oukan.2017.0_A-2-4.

Cho, S. (2022). CCDCOE. [online] *Tallinn 2022 National Cybersecurity Organisation: REPUBLIC OF KOREA.* Available at: https://ccdcoe.org/uploads/2022/12/ROK-Country-report.pdf [Accessed 9 May 2024].

Crandall, M. and Allan, C. (2015). *Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms. Contemporary Security Policy*, 36(2), pp.346–368. doi:https://doi.org/10.1080/13523260.2015.1061765.

Creswell, J.W. (2009). *Research Design : Qualitative, quantitative, and Mixed Methods Approaches.* 3rd ed. Los Angeles: Sage.

Crimson Japan (2020). 機械翻訳はここまで来た！*(Machine translation has come so far!).* [online] Japanese-English and English-Japanese translation services. Available at: https://www.crimsonjapan.co.jp/blog/where_machine_translation_has_reached/ [Accessed 11 May 2024].

Da-gyum, J. (2024). *S. Korea announces 'offensive cyber defence' strategy.* [online] The Korea Herald. Available at: https://www.koreaherald.com/view.php?ud=20240901050165 [Accessed 4 Dec. 2024].

Dewar, R. (2017). *ETH Library Active Cyber Defense*. CSS Cyberdefense Trend Analyses, [online] 1. doi:https://doi.org/10.3929/ethz-b-000169631.

DLA Piper (2024). *DATA PROTECTION LAWS OF THE WORLD Estonia.* [online] www.dlapiperdataprotection.com. DLA Piper . Available at: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=EE [Accessed 9 Aug. 2024].

Eisenhardt, K.M. (1989). *Building Theories from Case Study Research.* The Academy of Management Review, 14(4), pp.532–550. doi:https://doi.org/10.2307/258557.

Eom, T.Y. (2024). *AI and Cybersecurity in Digital Warfare on the Korean Peninsula.* [online] Georgetown Journal of International Affairs. Available at: https://gjia.georgetown.edu/2024/07/10/ai-and-cybersecurity-in-digital-warfare-on-the-korean-peninsula/ [Accessed 17 Jul. 2024].

e-Estonia. (2017). *How Estonia became a global heavyweight in cyber security — e-Estonia.* [online] Available at: https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/. [Accessed 9 May 2024]

e-Estonia. (2022). *Cyber security education in Estonia: from kindergarten to NATO Cyber Defence Centre.* [online] Available at: https://e-estonia.com/cybersecurity-education-in-estonia-from-kindergarten-to-nato-cyber-defence-centre/. [Accessed 9 May 2024]

Fukushima, G.S. (2006). *Japan's 'Soft Power'* 特集 日本のソフトパワー. 日本貿易会月報, [online] No.639. Available at: https://www.jftc.jp/monthly/archives/001/201802/9480ee77341ac62987618120e86cd807.pdf [Accessed 1 Dec. 2024].

Funabashi, Y. (2017). *Japanese strength in soft power foreign policy.* [online] The Soft Power 30. Available at: https://softpower30.com/japanese-strength-soft-power-foreign-policy/ [Accessed 1 Dec. 2024].

Haaster, J.V. (2016). *Assessing cyber power.* IEEE Xplore, [online] pp.7–21. doi:https://doi.org/10.1109/CYCON.2016.7529423.

Hankewitz, S. (2024). *Estonian e-residents contribute millions to the economy*. [online] Estonian World. Available at: https://estonianworld.com/business/estonian-e-residents-contribute-millions-to-the-economy/?utm_source=chatgpt.com [Accessed 21 Nov. 2024].

Harada, Y. (2022). *Competition over Cyber Norms Processes between a Norm Entrepreneur and a Norm Protector. National Institute for Defence Studies,* [online] 2(2). Available at: https://www.nids.mod.go.jp/publication/security/pdf/2022/202203_12.pdf [Accessed 10 Nov. 2024].

Hardy, A. (2024). *Estonia's digital diplomacy: Nordic interoperability and the challenges of cross-border e-governance*. Internet Policy Review, [online] 13(3). doi:https://doi.org/10.14763/2024.3.1785.

Hathaway, O.A. (2014). *The drawbacks and dangers of active defence.* doi:https://doi.org/10.1109/cycon.2014.6916394.

Herpig, S. (2023). *Active Cyber Defence Toward Operational Norms An analysis supported by the Transatlantic Cyber Forum*. [online] Available at: https://www.stiftung-nv.de/sites/default/files/snv_active_cyber_defence_toward_operational_norms.pdf [Accessed 12 May 2024].

Hidaka, T. and Ide, T. (2020). サイバーリザーブ（予備役）の研究 *(Study of Cyber Reserves)*. Maritime Academy Strategic Research Special Issue. [online]

Available at: https://www.mod.go.jp/msdf/navcol/assets/pdf/ssg2020_04_06.pdf [Accessed 9 May 2024].

Hoshiyama, T. (2008). 日本外交とパブリック・ディプロマシー：ソフトパワーの活用と対外発信の強化に向けて. [online] Institute for International Policy Studies. Available at: https://npi.or.jp/research/data/bp334j.pdf [Accessed 24 Nov. 2024].

Iasiello, E. (2023). *Active Defence May Lead to a More Weaponized Cyberspace.* [online] Available at: https://www.oodaloop.com/archive/2023/12/01/active-defence-may-lead-to-a-more-weaponized-cyberspace/ [Accessed 9 May 2024].

IISS. (2021). *Cyber Power – Tier Three.* [online] IISS. Available at: https://www.iiss.org/en/research-paper/2021/06/cyber-power---tier-three/ [Accessed 11 May 2024].

IISS (2023). *5. Estonia.* [online] Available at: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_05-estonia.pdf [Accessed 16 Dec. 2024].

Inoue, D. (2020). セキュリティ情報の自給に向けたサイバーセキュリティ知的基盤構想 *(The Cyber Security Intelligence Infrastructure Initiative for security information self-sufficiency).* [online] National Institute of Information and Communications Technology. Available at: https://www.soumu.go.jp/main_content/000683591.pdf [Accessed 9 May 2024].

Invest in Estonia. (n.d.). *Cyber Security.* [online] Available at: https://investinestonia.com/business-opportunities/cyber-security/overview/ [Accessed 9 May 2024].

ITU. (2020). *Global cybersecurity index 2020.* [online] Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

Jinnai, T. (2024). 自衛隊が行うサイバー作戦における情報法制上の課題. [online] Available at: https://lab.iisec.ac.jp/degrees/d/theses/iisec_d53_thesis.pdf [Accessed 12 Nov. 2024].

JPCERT/CC (2012). *TSUBAME* プロジェクト *(TSUBAME Project)*. [online] JPCERT/CC. Available at: https://www.jpcert.or.jp/tips/2012/wr124301.html [Accessed 12 May 2024].

JPCERT/CC (2021). サイバー攻撃被害情報の共有と公表のあり方について（公開版）. 令和2年度 総務省「サイバー攻撃の被害に関する 情報の望ましい外部への提供のあり方に係る調査・ 検討の請負」事業報告書. [online] Available at: https://www.soumu.go.jp/main_content/000762951.pdf [Accessed 18 Nov. 2024].

Kan, H. (2022). *Korea eyes world No. 3 spot in digital competitiveness by 2027.* [online] The Korea Herald. Available at: https://www.koreaherald.com/view.php?ud=20220928000706 [Accessed 8 Dec. 2024].

Kallender, P. and Hughes, C.W. (2016). *Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace.* Journal of Strategic Studies, 40(1-2), pp.118–145. doi:https://doi.org/10.1080/01402390.2016.1233493.

Kaska, K., Osula, A.-M. and Stinissen, J. (2013). *The Cyber Defence Unit of the Estonian Defence League Legal, Policy and Organisational Analysis.* [online] NATO CCDCOE. Available at: https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf. [Accessed 9 May 2024].

Katzenstein, P.J. (1996). *Cultural Norms and National Security Police and Military in Postwar Japan.* Cornell University Press.

Kelley, J.G. and Simmons, B.A. (2014). *Politics by Number: Indicators as Social Pressure in International Relations.* American Journal of Political Science, 59(1), pp.55–70. doi:https://doi.org/10.1111/ajps.12119.

Kim, D.-H. (2013). *Coercive Assets? Foreign Direct Investment and the Use of Economic Sanctions.* International Interactions, 39(1), pp.99–117. doi:https://doi.org/10.1080/03050629.2013.751305.

Kim, F. (2024). *South Korea launches defence AI center to enhance technology capabilities.* [online] Ipdefenceforum.com. Available at: https://ipdefenceforum.com/2024/07/south-korea-launches-defence-ai-center-to-enhance-technology-capabilities/ [Accessed 3 Dec. 2024].

Kim, M. (2022). *The Growth of South Korean Soft Power and Its Geopolitical Implications.* JOURNAL OF INDO-PACIFIC AFFAIRS , [online] 5(2576-5361), pp.P.123-138. Available at: https://media.defence.gov/2022/Nov/08/2003110774/-1/-1/1/_JIPA%20KOREA-SPECIAL%20ISSUE%202022.PDF [Accessed 5 Dec. 2024].

Kim, S.G. (2015). 韓国のサイバーセキュリティ人材資源への投資 *- CODE BLUE 2015.* [online] Available at: https://www.slideshare.net/slideshow/by-seungjoo-gabriel-kim-code-blue-2015/59669523#28 [Accessed 8 Dec. 2024].

Kim, S.J. and Bae, S. (2021). *Korean Policies of Cybersecurity and Data Resilience* . The Korean Way With Data How the World's Most Wired Country Is Forging a Third Way, [online] p.p. 39-60. Available at: https://carnegie-production-assets.s3.amazonaws.com/static/files/202108-KoreanWayWithData_final5.pdf [Accessed 20 Dec. 2024].

KISA (2021). *Global Activites: GCCD.* [online] www.kisa.or.kr. Available at: https://www.kisa.or.kr/EN/201 [Accessed 6 Dec. 2024].

Kohler, K. (2020). *CYBERDEFENSE REPORT Estonia's National Cybersecurity and Cyberdefence Posture Policy and Organizations.* CSS Cyberdefence Reports. [online] doi:https://doi.org/10.3929/ethz-b-000438276.

Kshetri, N. (2014). *Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses.* East Asia, [online] 31(3), pp.183–201. doi:https://doi.org/10.1007/s12140-014-9215-1.

Kuehl, Daniel T.(2009) *"From Cyberspace to Cyberpower: Defining the Problem." In Cyberpower and National Security.* Washington, D.C.: National Defence University Press.

Kumagai, K. (2021). *世界最先端のIT国家、エストニアを知っていますか【第6回】IT教育とスマートシティーから見る変革の仕組み｜お役立ち情報｜ユニアデックス株式会社.* [online] UNIADEX ユニアデックス株式会社. Available at: https://www.uniadex.co.jp/column/annex-security/usefulinfo/estonia_6.html [Accessed 9 May 2024].

Kurosaki, M. (2023). 能動的サイバー防御の国際法枠組み—武力未満と違法性阻却による正当化の可能性—. 国際問題, [online] No. 716. Available at: https://www2.jiia.or.jp/kokusaimondai_archive/2020/2023-12_004.pdf?noprint [Accessed 1 Dec. 2024].

Kwak, Y. (2024). *NK's Lazarus hacked South Korean top court: police.* [online] koreatimes. Available at: https://www.koreatimes.co.kr/www/nation/2024/04/103_369976.html#:~:text=According%20to%20the%20NIS%2C%2080 [Accessed 12 May 2024].

Lee , S. and Lee , J. (2024). *Concerns arise as S. Korea transfers espionage authority to police.* [online] The Chosun Daily. Available at: https://www.chosun.com/english/national-en/2024/01/02/BMICXDGAVFAZ5ACX4WSWDQF65Q/ [Accessed 5 Dec. 2024].

Matsubara. M (2022) Asia Pacific Initiative [online] 日本は「ハイブリッド戦争」の脅威に備えているか *(Is Japan ready for the threat of hybrid war?)*. Available at: https://apinitiative.org/2022/08/08/39255/. [accessed 9 May 2024]

Matsubara, M., Yamaguchi, R. and Koizumi, Y. (2022). ウクライナにおける戦争からの教訓 サイバーなどでの各国の動き（下）. [online] 新潮社 Foresight(フォーサイト). Available at: https://www.fsight.jp/articles/-/49199 [Accessed 20 Oct. 2024].

Matsumura, M. (2022). 我が国のサイバーセキュリティ戦略の欠点と展望 —「平和国家」体制の桎梏への対応を考える. Journal of Information and Communications Policy, Vol.5(No.2), p.Pages 73-94. doi:https://doi.org/10.24798/jicp.5.2_73.

Mattson, T. (2018). *Guaranteeing the safety of critical databases requires considerably more care.* [online] Riigikontroll.ee. Available at: https://www.riigikontroll.ee/Suhtedavalikkusega/Pressiteated/tabid/168/ItemId/995/amid/557/language/en-US/Default.aspx [Accessed 15 Nov. 2024].

Merriam, S.B. (2009). *Qualitative Research: A Guide to Design and Implementation.* San Francisco: Jossey-Bass.

Misumi, I. (2020). サイバーセキュリティ基本法制定・改正の経緯 *(The background of enactment and amendment of the Basic Act on Cybersecurity)*. Japan Society of Security Management Journal, 34(1), pp.28–34. doi:https://doi.org/10.32230/jssmjournal.34.1_28.

MOD. (2019). Ministry of Defence, Self-Defence Forces｜防衛白書｜*1* 防衛関係費の概要 *(Defence White Paper ｜1 Outline of Defence Expenditures).* [online] www.clearing.mod.go.jp. Available at: http://www.clearing.mod.go.jp/hakusho_data/2019/html/n24301000.html [Accessed 11 May 2024].

MOD. (2021). *Japan Ministry of Defence.* [online] Japan Ministry of Defence. Available at:

https://www.mod.go.jp/en/article/2021/04/5fd96950ea91fddb91d84033407c1f9b16d95378.html [Accessed 24 Nov. 2024].

MOD (2022). 防衛省・自衛隊｜令和*4*年版防衛白書｜＜解説＞自衛隊サイバー防衛隊の新編について. [online] Mod.go.jp. Available at: https://www.mod.go.jp/j/publication/wp/wp2022/html/nc007000.html [Accessed 15 Dec. 2024].

Mori, T. (2016). 新安保法制と国際法上の集団的自衛権 *(New Security Legislation and the Right of Collective Self-Defence under International Law)*. International Issues, [online] 648(2) p6-15. Available at: https://www2.jiia.or.jp/kokusaimondai_archive/2010/2016-01_002.pdf?noprint.

Nakashima, E. (2023). *China hacked Japan's sensitive defence networks, officials say.* Washington Post. [online] 8 Aug. Available at: https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/.

Nakatani, K. (2024). *Japan's cyber defence and it's challenges.* 13 May. Personal interview via online conversation.

Nikkei Newspaper. (2023). 防衛大学校にサイバー学科、*27*年度にも 幹部候補を養成 *(Cyber Department to be newly established at the National Defence Academy, to train candidates for military officers in FY27)*. [online] Nikkei Newspaper. Available at: https://www.nikkei.com/article/DGXZQOUA2773Q0X21C22A2000000/ [Accessed 11 May 2024]

NISC. (n.d.). *About NISC.* [online] www.nisc.go.jp. Available at: https://www.nisc.go.jp/eng/index.html [Accessed 11 May 2024].

NISC (2020). サイバーセキュリティに係る人材の確保、育成、活躍の促進 付加価値の高い仕事をする. [online] Available at:

https://www.nisc.go.jp/pdf/council/cs/jinzai/dai13/13shiryou0102.pdf [Accessed 26 Nov. 2024].

Nishimura, I., Ikeda, S. and Tagami, K. (2023). 雇用流動化と日本経済　ホワイトカラーの採用と転職. 労働政策研究・研修機構.

Nomura, A. (2020). 韓国のデジタル・ガバメント —行政改革と一体となった中央集権・組織横断型の取り組み—. Research Focus, [online] No.2020-034, pp.pp.10-12. Available at: https://www.jri.co.jp/MediaLibrary/file/report/researchfocus/pdf/12305.pdf [Accessed 20 Dec. 2024].

Nye, J.S. (2004). 日本のソフト・パワー--その限界と可能性 (特集 クール・ジャパン--国力の根源に迫る). 外交フォーラム, 17(6), pp.12–15.

Nye, J.S. and Belfer Center For Science And International Affairs (2010). *Cyber power.* Cambridge, Ma: Harvard Kennedy School, Belfer Center For Science And International Affairs.

Nye, J.S. (2011). *The future of power.* New York: Public Affairs.

OECD. (2019) OECD Economic Surveys: Japan 2019.Publishing, Paris, P 39. Available from: OECD iLibrary, https://doi.org/10.1787/fd63f374-en.

Oguma, K. (January 22, 2024). 日本は*11*万人不足「セキュリティ人材」確保の難題 [online] Toyokeizai Online. Available at: https://toyokeizai.net/articles/-/727210 [Accessed 12 May 2024].

Osawa, J., Kaska, K., Rebane, L., Vaks, T., Osula, A.-M. and Komiyama, K. (2021). So *Far, Yet So Close: Japanese and Estonian Cybersecurity Policy Perspectives and Cooperation* Japanese and Estonian Cybersecurity Policy Perspectives and Cooperation on JSTOR. Jstor.org, [online] (2228-0529). doi:https://doi.org/10.2307/resrep54440.

Park, J.H. and Reddy, S. (2024). *South Korea unveils new cyber strategy to counter North Korean threats* | NK News. [online] NK News - North Korea News. Available at: https://www.nknews.org/2024/02/south-korea-unveils-new-cyber-strategy-to-counter-north-korean-threats/ [Accessed 12 Nov 2024].

Parliament of Estonia (2018). Cybersecurity Act–Riigi Teataja. [online] www.riigiteataja.ee. Available at: https://www.riigiteataja.ee/en/eli/523052018003/consolide [Accessed 16 Dec. 2024].

Pau, A. (2018). *Tehtud! Eesti kaitsevägi lõi küberväejuhatuse.* [online] Tehnika. Available at: https://tehnika.postimees.ee/6026027/tehtud-eesti-kaitsevagi-loi-kubervaejuhatuse [Accessed 4 Dec. 2024].

Polkinghorne, D.E. (2005). *Language and meaning: Data collection in qualitative research*. Journal of Counseling Psychology, 52(2), pp.137–145. doi:https://doi.org/10.1037/0022-0167.52.2.137.

Põldma, L. (2021). *IT students have an opportunity to pass military service in the Cyber Command.* [online] Education Estonia. Available at: https://www.educationestonia.org/education-cybersecurity-military-service/ [Accessed 11 Dec. 2024].

RIA (2020). *Cyber Security In Estonia 2020 2 CYBER SECURITY IN ESTONIA 2020.* [online] RIA. Available at: https://www.ria.ee/sites/default/files/documents/2022-11/Cyber-Security-in-Estonia-2020.pdf [Accessed 15 Dec. 2024].

RIA. (2022). *Cyber defence of critical infrastructure* | RIA. [online] www.ria.ee. Available at:

https://www.ria.ee/en/cyber-security/cyber-defence-critical-infrastructure/cyber-defence-critical-infrastructure [Accessed 11 May 2024].

Robinson, N., Kask, L. and Krimmer, R. (2019). *The Estonian Data Embassy and the Applicability of the Vienna Convention. International Conference on Theory and Practice of Electronic Governance*, p.p. 391-396 doi:https://doi.org/10.1145/3326365.3326417.

Rowland, J., Rice, M. and Shenoi, S. (2014). *The anatomy of a cyber power.* International Journal of Critical Infrastructure Protection, [online] 7(1), pp.3–11. doi:https://doi.org/10.1016/j.ijcip.2014.01.001.

Sakurada, D. (1998). *Why we need the US-Japan security treaty.* Asia-Pacific Review, 5(1), pp.13–38. doi:https://doi.org/10.1080/13439009808719961.

Security News. (2021). 日本語に守られてきた時代は終わった。今後、激化するサイバー攻撃から身を守る手段とは。*(The era of protection by the Japanese language is over. What are the means of protection against cyber-attacks that will intensify in the future?).* [online] Available at: https://securitynews.so-net.ne.jp/topics/sec_20188.html [Accessed 9 May 2024].

Shiy, Tao. (2020). *Learning from the 'Miracle of Han River'.* International Journal of Contemporary Research and Review, 11(05). doi:https://doi.org/10.15520/ijcrr.v11i05.809.

Sohta, Y. (2024). *身代金を支払わない結果、日本のランサムウェア感染率は減少？ ランサムウェア感染率/身代金支払率15か国調査 2024* | Proofpoint JP. [online] Proofpoint. Available at: https://www.proofpoint.com/jp/blog/threat-insight/japan-ransomware-payment-result-2024 [Accessed 20 Oct. 2024].

Song, T.E. (2023). *Latest Developments in North Korea's Cyber Aggression and the ROK's Responses.* [online] Ifans.go.kr. Available at:

https://www.ifans.go.kr/knda/ifans/eng/pblct/PblctView.do?csrfPreventionSalt=null&pblctDtaSn=14198&menuCl=P11&clCode=P11&koreanEngSe=ENG [Accessed 4 Dec. 2024].

StartHome. (2022). １５年前の「戦争」糧に＝サイバー防衛で世界リード―専門家育成へ英才教育・エストニア *(Learning from the 'war' of 15 years ago - Leading the world in cyber defence - Elite education to foster experts, Estonia).* [online] Available at: https://home.kingsoft.jp/news/news/jiji/2022120300329.html?from=recent_v2_news [Accessed 9 May 2024].

TBS NEWS DIG. (2024). 日本のセキュリティはマイナーリーグ「能動的サイバー防御」って何？*(Japanese security is in the minor leagues. What is 'active cyber defence'?).* [online] Available at: https://newsdig.tbs.co.jp/articles/-/1075990?page=3 [Accessed 12 May 2024].

The Cabinet Office of Japan. (2022).「個人情報保護法」をわかりやすく解説　個人情報の取扱いルールとは？*(The 'Personal Information Protection Law' explained in an easy-to-understand manner What are the rules for handling personal information?).* [online] Government Public Relations Online. Available at: https://www.gov-online.go.jp/useful/article/201703/1.html [Accessed 12 May 2024].

The Cabinet Office of Japan. (2024). 有事などの際、国を支える力になる！「予備自衛官等制度」*(You can help the country in case of an emergency! 'Reserve Self-Defence Forces Officers System').* [online] Government of Japan Public Relations Online. Available at: https://www.gov-online.go.jp/useful/article/201405/2.html#fourthSection [Accessed 9 May 2024].

The Government of Estonia (2023). *Benefit from the e-Residency community in 4 key ways.* [online] e-Residency. Available at:

https://www.e-resident.gov.ee/blog/posts/benefit-from-the-e-residency-community / [Accessed 21 Nov. 2024].

The Government of Japan. (1947). 日本国憲法 *(The Constitution of Japan).* [online] elaws.e-gov.go.jp. Available at: https://elaws.e-gov.go.jp/document?lawid=321CONSTITUTION_19470503_000000000000000&keyword=%E6%97%A5%E6%9C%AC%E5%9B%BD%E6%86%B2%E6%B3%95 [Accessed 11 May 2024].

The Government of Japan. (2018). サイバーセキュリティ基本法 *(The Basic Act on Cybersecurity).* [online] elaws.e-gov.go.jp. Available at: https://elaws.e-gov.go.jp/document?lawid=426AC1000000104_20220617_504AC0000000068&keyword=%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E5%9F%BA%E6%9C%AC%E6%B3%95 [Accessed 11 May 2024].

The White House. (2011). *INTER NATIONA L STR ATEGY FOR CYBERSPACE: M A Y 2 0 1 1 Prosperity, Security, and Openness in a Networked World.* [online] Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Accessed 27 Nov. 2024].

Uesugi, K. (2018). 「韓国のサイバーセキュリティ政策の現状」*(The State of South Korea's Cybersecurity Policy).* [online] Japan Cyber Security Innovation Committee. Available at: https://www.j-cic.com/column/SouthKorea-Cybersecurity-Policy.html [Accessed 9 May 2024].

Uesugi, K. and Hirayama, T. (2018). 諸外国におけるサイバーセキュリティの情報共有に関する調査 (Survey on Information Sharing on Cyber Security in Other Countrie). [online] Japan Cybersecurity Innovation Committee (JCIC). Available at:

https://www.j-cic.com/pdf/report/CybersecurityInformationSharingSurvey-20180309(JP).pdf [Accessed 11 May 2024].

UN. (1945). *UN Charter.* [online] United Nations. Available at: https://www.un.org/en/about-us/un-charter.

Valeriano, B. and Leasure, Q. (2024). *The Limits of Soft Power: South Korea Joins the Great Power Game.* [online] The National Interest. Available at: https://nationalinterest.org/blog/korea-watch/limits-soft-power-south-korea-joins-great-power-game-213652 [Accessed 2 Dec. 2024].

Vosse, W. (2024). *Japan’s gradual shift from passive to active cyber defense: Evidence from the domestic discourse and international cooperation*. Deleted Journal, N° 2(1), pp.89–106. doi:https://doi.org/10.3917/efrc.232.0089.

Yamaguchi, Y. (2019). *Strengthening Public-Private Partnership in Cyber Defence: A Comparison with the Republic of Estonia.* NIDS Journal of Defence and Security, [online] 20(ISSN 2186-6902), pp.67--111. Available at: https://www.nids.mod.go.jp/english/publication/kiyo/pdf/2019/bulletin_e2019_4.pdf [Accessed 12 Nov. 2024].

Yamazaki, F. (July 28, 2023). サイバー警察官が一堂に会する ″白浜シンポジウム. | Net One Systems. [online] Available at: https://www.netone.co.jp/media/detail/20230728-01/ [Accessed 9 May 2024].

Yin, R.K. (2018). *Case Study Research and Applications: Design and Methods.* 6th ed. Thousand Oaks, California: Sage Publications.