Leiden University – Faculty of Governance and Global Affairs

Master Thesis

An Assessment of International Cyber Security Policy:

Middle Power Agility in The Netherlands and South Korea

Name: Ruben Levy

Student number: S1570935

Program: MSc Crisis and Security Management

Supervisor: Dr. Jan Melissen

Second reader: Dr. mr. Ernst Dijxhoorn

Date: 04-08-2019

Word Count: 18.679

Table of contents

Acknowledgements

I would like to express my appreciation for my supervisor dr. Jan Melissen, who provided me with insightful feedback and ideas. His flexible attitude allowed me to complete this project at my own pace irrespective of my whereabouts. Jan, I thank you for allowing me to finalise this thesis project from the other side of the world. Also, I thank Sico van der Meer with special gratitude for proving me with fundamental information during a lengthy interview at the Clingendael Institute. The fruitful conversation has served as a cornerstone for my thesis. Furthermore, I would like to thanks second reader dr.mr. Ernst Dijxhoorn for his corrections and final assessment of this piece. And lastly a great word of gratitude to my parents, brother and friends that have pulled me through the more difficult moments of ample inspiration I have encountered along the way.

List of abbreviations

AIVD:	General Intelligence and Security Service
APT:	Advanced Persistent Threat
ASEAN:	Association of Southeast Asian Nations
CAMP:	Cybersecurity Alliance for Mutual Progress
CERT:	Cyber Security Emergency Response Team
CSAN:	Cyber Security Assessment Netherlands
DCSA:	Dutch Cyber Security Agenda
DCS:	Defence Cyber Strategy
DDoS:	Distributed Denial-of-Service Attack
DNS:	Domain Name System
EU:	European Union
GCSI:	Global Cyber Security Index
GFCE:	Global Forum on Cyber Expertise
IFSS:	Integrated Foreign and Security Strategy
ICS:	International Cyber Strategy
ICT:	Information and Communications Technology
IR:	International Relations
ITU:	United Nations International Telecommunications Union
KISA:	Korea Internet and Security Agency
KnCERT/CC:	Korean Computer Emergency Response Team/ Coordination Center
MIVD:	Military Intelligence and Security Service
MIKTA:	An informal partnership between Mexico, Indonesia, South Kora, Turkey and Australia
MND:	Ministry of National Defence
NAPCI:	Northeast Asia Peace and Cooperation Initiative
NATO:	North Atlantic Treaty Organisation
OECD:	Organisation for Economic Co-operation and Development
SDD:	Seoul Defense Dialogue
USA:	United States of America

Introduction

In 2007, large-scale cyber-attacks ruptured Estonian critical infrastructure. Stemming from ethnic tensions, Russian-speaking minorities inside the state carried out the attacks in reaction to a decision by the Estonian government to relocate a monument commemorating the Soviet liberation after World War II from a central location in Tallinn to a military cemetery. In the period between the 27th of April and the 18th of May, a multitude of distributed denial-of-service (DDoS) attacks targeted Estonia's central infrastructure and paralysed banks, political parties and even shut down most government websites.[1] Due to technical considerations surrounding such attacks, attribution remains almost impossible. However, it remains clear that the Kremlin supported the cause of the hackers their direct involvement has not been found, not by the European Commission nor by the North Atlantic Treaty Organisation (NATO).[2] Nonetheless, for the Russian minority it demarcated a decline in ethnic identity, accordingly it did not only strain bilateral relations between Russia, it also marked the first public large-scale cyberattacks in history.[3]

This thesis project will focus on this current era wherein cyber evoked a new place next to the traditional domains of warfare by conducting a case study on The Kingdom of the Netherlands (The Netherlands) and The Republic of Korea (South Korea). Cyber space is fundamentally different from land, sea air or space as it cannot be entered and consists of bits and bytes, the availability of resources and sheer state size still largely decides which states dominate it. Even more so because most of the infrastructure needed, such as the Domain Name System (DNS) is controlled by a handful of private actors from those great power states.[4]

The position of states in the cyber power debate remains insecure. This thesis will add to the existing literature on middle power states by executing two case studies wherein the agility of middle power states will be assessed through an assessment of agility, measured through systemic impact. The following research question will be answered:

How does the prioritization of cyber security policies affect the agility of The Netherlands and South Korea as middle powers in the international environment?

[1] Herzog, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses', 50–51.
[2] Herzog, 50–51.
[3] Herzog, 50–51.
[4] McGuffin and Mitchell, 'On Domains', 409.

In International Relations (IR), middle power theory dictates that medium-sized states that focus their resources on specific policy areas can enlarge their power in these areas despite of their more limited resources in comparison to great powers. Having less resources than great power states, policymakers in middle power states have to make specific choices in which direction to steer domestic and foreign policy to create more influence in certain policy areas over others. These specific policy directions, or niches, are telling for middle power foreign policy as it is impossible to focus on all areas as is the case in great power politics.[5] In this line of reasoning, similar questions have been researched regarding power issues regarding military or economic power, however no such study has been conducted regarding cyber power yet. This study will focus exclusively on the cyber realm by using theoretical underpinnings regarding cyber power by Dr. David Betz and Dr. Tim Stevens.[6]

A limited number of scholars have developed models to delve deeper into the subject of cyber power. Robert Nye focussed on three faces of power where he focussed on direct power, power issues in relation to political decision-making and lastly the notion of soft power.[7] In turn, Alexander Klimburg focusses for a large part on strong defensive cyber capacities, sometimes out of the context of direct national interests.[8] Both models offer and elaborate tool to display the presence of cyber power in states. However, both models focus on direct forms of cyber power while they lack a vital point regarding diffuse power which manifests itself through the construction of social relations.[9] The 'dimensions model' by Betz and Stevens does include this important factor and thus will be used for this thesis project.

Betz and Stevens, both professors at Kings College London, specialised in among others war studies and cyber security, developed an effective framework which enables the user to explain both direct and indirect manifestations of cyber power which are both fundamental in order to provide an answer to the research question. In other words, the findings will serve as a graduator for cyber power and will highlight the extent to which middle powers have manoeuvring space next to more resourceful states in cyber space. The findings will eventually serve as the basis for the embellishment of agility. Hereby, statements can be made regarding cyber power and its effect in medium-sized states by using this specific framework by Betz and Stevens.

[5] Sico van der Meer, Cyber power in The Netherlands and South Korea.
[6] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*.
[7] Nye, *Cyber Power*.
[8] Klimburg, 'The Whole of Nation of Cyberpower International Engagement on Cyber Establishing International Norms and Improved Cybersecurity'.
[9] Myriam Dunn Cavelty, 'Europe's Cyber-Power', 308.

It is important to note down in the beginning of this thesis that agility is a concept that has no academic precedents. Hence, it has not been used by academics before to describe the process of an increasing or decreasing manoeuvring space in a middle power's policy objectives. In this thesis, agility will take on this conceptualisation. To be more precise, agility in the cyber realm explores the extent to which an independent course of action can be adopted by specifically middle powers in light of its geostrategic situation and great power politics. In order to establish agility in the Netherlands and South Korea, the findings that stem from the dimensions model of cyber power will be used to establish systemic impact. This will be elaborated on in the methodology section. In brief, systemic impact sheds light on concrete forms of cyber power by combining the three elements as described by Betz and Stevens, eventually leading to an elaborate assessment of manoeuvring space, or agility of middle powers in specifically the cyber realm.

Before the two cases are introduced, it is relevant to point out that most of the analysis done in this thesis is limited to the cyber realm where a multiplicity of factors is left undiscussed due to the scope of this project. The Netherlands has had a gradual growth in its international foreign policy ambitions after World War II, with the emergence of multilateralism, the United Nations, the NATO and European Coal and Steel Community where it has advanced its interests of a multilateral global order since then. One could argue that cyber is merely a logical next step in this policy.[10] South Korea, in turn, has undergone a different development where its multilateral embeddedness has only developed in recent decades, such as its introduction to the Group of Twenty (G20) and the establishment of MIKTA in 2013, as an informal partnership between Mexico, Indonesia, South Kora, Turkey and Australia to spread cross-regional mutual norms.[11] MIKTA is especially telling for South Korea's multilateral development because it is one of the first tools where South Korea has used public diplomacy as a reinforcement of its foreign policy interests.[12]

Parallels exist between the Netherlands and South Korea in their effort to enhance multilateral cooperation regarding the advancement of human rights, economic policy and political liberties.[13] In addition, a multi-stakeholder model in international affairs is propagated by both states. With regards to the cyber realm, the Netherlands and South Korea are such middle

[10] de Wijk, 'Een Kompas Voor Een Wereld in Beweging: De Rol van Buitenlandse Zaken in Het Borgen van Nederlandse Belangen', 13.
[11] Lee, 'New Approach of South Korea's Middle Power Diplomacy: Focusing on Global Agenda Setting', 43.
[12] Melissen and Sohn, 'Leveraging Middle Power Public Diplomacy in East Asian International Relations', 24 November 2015, 3.
[13] Sico van der Meer, Cyber power in The Netherlands and South Korea.

powers that focus considerably on cyber power. The decision to focus in this niche has different origins for both states. The choice for these two specific, democratic middle powers originates from the fact that both invest considerable resources into international cyber-security diplomacy initiatives.

In more detail, the Netherlands focusses on the strengthening of international cooperation and dialogue regarding the strengthening of cyber-capacities of other states. An example is the fourth Global Conference on Cyberspace that took place in 2015 and its Ministry of Foreign Affairs initiated The Hague process in order to ensure transparency during the drafting of the Tallinn Manual. In turn, South Korea, entered the cyber debate for multiple other reasons. Firstly, the occurrence of a large-scale cyber-attack in 2009 carried out by North-Korea rigorously displayed the urge for increased cyber defence. Secondly, South Korea's focus on digitalization of the society and a developed high-tech sector which is closely linked to economic development have made cyber power a natural priority.[14][15] With regards to cyber, South Korea hosts the annual Seoul Defense Dialogue (SDD) where cyber security technical advancement and confidence-building are of paramount importance.[16]

Lastly, when comparing these kind of initiatives, it is important to differentiate between traditional security issues and an asymmetric inter-network issue such as cyber security issues.[17] As the process of the impression of fundamental norms and the encapsulating of cyber security in international frameworks, it is to be seen how said initiatives will contribute to the advancement of cyber power for both cases.

Research question

By executing a dual case-study the aim of this project is to test indicators that map the extent of cyber power in middle power states and hereby add to middle power theory especially focussed on the cyber realm by executing a systemic impact analysis. In the research question as stated in the introduction, agility reflects the ability for middle powers to follow an alternative path on the cyber realm than their great power allied states through systemic impact. Also, this conceptualisation will be operationalised in more detail in the methodology section. Middle power states are especially susceptible to global trends and changes in comparison to great

[14] Melissen and de Keulenaar, 'Critical Digital Diplomacy as a Global Challenge', 298.
[15] Campbell, 'Building an IT Economy: South Korean Science and Technology Policy', 1–4.
[16] Sico van der Meer, 'Medium-Sized States in International Cyber Security Policies', 4–5.
[17] Sangbae Kim, 'Policy Recommendation for Cyber Security South Korea's Middle Power Diplomacy:', 3.

powers and emerging great powers such as Brazil and India. Growing economic and diplomatic pressure by those emerging states have made the manoeuvring space of middle power states increasingly limited. In addition, small states such as Singapore and Qatar take increasing their influence from the other side of the spectrum using national branding strategies. In line with Andrew Cooper, it is therefore necessary to reassess the position that middle powers hold in international power politics.[18]

Objective

Following from the relevance of this research flows a clear objective. This project aims to add onto the existing literature regarding middle power states by conducting a dual case study on The Netherlands and South Korea and hereby answering the research question. In this sense, middle power theory will be critically assessed by reviewing the two cases in an attempt to add to middle power theory, when applied to the cyber realm by using agility as a graduator. Herein the conclusion will shed light on the question hoe middle power theory reflects on the cyber realm. It must be noted that the cyber debate is too broad to be discussed in its entirety. Therefore, the objective of this thesis is to zoom in to cyber capabilities from a state centred perspective. The choice to exclude non-state actors from the analysis had been made decisively.

Structure

This project will be structured in the following manner; the next chapter, the theoretical framework will highlight the relevant aspects of middle power theory which are essential to answer the research question. Afterwards, the methodology and research design chapter will justify the case selection and scope of the research. Furthermore, a model will be presented with which the two cases will be analysed on their cyber power capacities following the article by Betz and Stevens. The model will be applied to the two cases individually in order to allow for a general analysis of agility in middle power states through establishing systemic impact. In the final part of this project the systemic impact of cyber power will demonstrated in both cases after which these finding will be used to shed new light on middle power theory focussing on cyber security.

[18] Andrew F. Cooper, 'Middle Powers: Squeezed Out of Adaptive', 29–30.

Theoretical Framework

The discussion revolving around middle power states in International Relations requires careful nuance. The definition of a middle power states is not set in stone. The following chapter will elaborate on the working definition of said concept and the accompanying theoretical underpinnings. Furthermore, fundamental concepts such as agility, niche diplomacy, hard- and soft power, cyberspace and cyber security will be defined in the scope of this project in order to enable it to apply them to the cases in an unambiguous manner. Lastly the current research project will be positioned in middle power theory. Middle power theory stems from IR where its definition is heavily disputed. This section aims to shed light on the definition of middlepowermanship what will be used in this project by highlighting the theoretical foundation and establishing the working definition applicable to both cases; the Netherlands and South Korea.

Middle power theory

Before delving into middle power theory is important to note that the concepts of hard- and soft power are relevant for middle power theory because middle powers focus on specific policy areas. Herein, the application of hard- or soft power can result in different outcomes, especially relating to their agility as will be explained later on. Having coercive, hard power capabilities in one policy area does not automatically mean it can be transferred to another, highlighting the importance of the application of soft power tactics. Lastly it is important to note that power is a relative and comparative concept, it can only be established in relation to another actor. Relative power is always measured in relation to other actors and power relationships can change over time.[19] For the Netherlands and South Korea this means in practice that they are less powerful than the United States of America but more powerful than Malta. Now the fundament of power theory is elaborated upon, the next section will delve deeper into middle power theory.

To start off, it is important to emphasize the fact that the used of the term middle power is relatively new in IR. Notwithstanding its historical context, which can be traced back to the sentiment that states should be defined more concretely besides classifying them as merely ‘large’ or ‘small’, contemporary use of the term middle power emerged at the close of World

[19] Eytan Gilboa, ‘The Public Diplomacy of Middle Powers: Navigating the Middle’, 22.

War II. Around this time, Canadian and Australian leadership aspired to play a more pronounced role in global reconstruction, highlighting distinct differences between them as frontrunners in efforts to restore the global world order.[20] As both states could not compete with the great powers back then, the term middle power came into existence in order to classify states that were more dominant in certain policy areas than others. In essence, all definitions that are given in the literature are controversial in some way, which makes it necessary to define the term in the context of this project.[21]

From an academic point of view, scholars have drafted various definitions, the most relevant ones will be discussed briefly in a chronological order. In the post-Cold War era Andrew Cooper, Richard Higgott and Kim Nossal categorised middle powers, mainly using a behaviour-based definition, where middle powers can be recognised by their foreign policy choices.[22] They divided the term into a positional, geographic, normative and a behavioural aspect. The positional aspect relates to the material capacity that a state holds in the international system. The geographic aspect of middlepowermanship relates to both the geographical and ideological position of middle powers in between great power states. Lastly, the normative aspect discussed the extent to which as middle power serves as an international broker or facilitator on the global stage while not taking up the role of the hegemon.

Later on, Cooper, Higgott and Nossal added the behavioural component to their definition. This aspect focusses on the diplomatic ambitions of middle powers. Most important in this aspect is that middle powers emphasise multilateral solutions to problems wherein consensus is achieved between the different stakeholders.[23] In order to nuance the view of Cooper, Higgot and Nossal, it is important to elaborate on the fact that such behavioural definitions are inextricably rooted in the political biases of that time, in this case, the post-Cold War period.[24]

More recent definitions stem from, among others, Andrew Carr and Eduard Jordaan. In 2014, Andrew Carr updated the definition of middle power states as used by Cooper, Higgot and Nossal. He identified three categories, position, behaviour and identity and based his definition on these previous findings by scholars.[25] The position approach aims to rank middle powers in an objective manner. This quantitative approach is then used to capture states that are small nor large when comparing the indicators as set in figure 1. More specifically middle powers are

[20] Robertson, 'Middle-Power Definitions', 357–58.
[21] Carr, 'Is Australia a Middle Power?', 70.
[22] Robertson, 360.
[23] Robertson, 360.
[24] Robertson, 364.
[25] Carr, 'Is Australia a Middle Power?', 71–77.

expected to rank among the first twenty states when ranked on these indicators according to Carr. Establishing middlepowermanship on the position approach alone is not enough as it does not account for what the difference in indicators means in essence. In addition, focussing in the positional approach alone results in a thinking process focussed on averages instead of the strategic position of a state.[26]

Following the position approach, Carr notes that the behavioural approach focussed on a diplomatic policy of brokering and 'good international citizenship. This implies that states can be considered middle powers then they act like one. Hereby the criticism is that there is no real background to test the middlepowermanship against as is the case with the position approach that uses clear indicators.[27] Ultimately, the identity approach to middlepowermanship as described by Carr views middle powers as a constructed political category. This is a less popular definition as it views middlepowermanship as a mere tool to provide the state with the assumed positive associations that come with using the term. Consequently, when middle power status is claimed by policymakers, it is telling for the way in which it will act in the international arena. On the other hand, this definition allows for a constant shift in being a middle power or not when the term is used in certain periods by policy makers and left out in others. This is a widespread notion in establishing identity in the constructivist tradition.[28]

Category	Indicators	Goal
1 Position: *Quantifiable factors*	- GDP, population, military size, defence spending	An objective ranking of state size
2 Behaviour: *Focus on how middle powers act on the international stage and guide their diplomacy*	- Membership in UNHRC or UNSC - size of diplomatic network	Striving for multilateralism, 'good international citizenship'
3 Identity: *Middlepowermanship as a constructed political category, a state's own use of the label*	- actual investment in reliable self-image (UNDP and FHI)	Achieving positive associations, international prestige

Figure 1: Three categories to define middle powers.[29]

[26] Carr, 72.
[27] Carr, 74.
[28] Finnemore and Sikkink, 'Taking Stock: The Constructivist Research Program in International Relations and Comparative Politics', 399.
[29] Carr, 'Is Australia a Middle Power?', 71–77.

A combination of these three elements offer an elaborate way to determine which states qualify as a middle power. Again, there is no conclusive definition and in isolation all three categories would prove insufficient. Considered in unison, it offers a complete picture of middle power status. Hence, the model as described above will be used to demonstrate the middle power position of The Netherlands and South Korea.

Ultimately, it is important to note that Carr offers an alternative way of establishing middlepowermanship. The *systemic impact approach* states that middle powers should be able to protect their vital interests and initiate change in the international order through formalised structures and informal channels such as the imposition of norms.[30] Systemic impact will be examined in the analysis of both cases by focussing on cyber power by using a model, which will be elaborated upon in the methodology section in order to eventually assess agility. By applying the systemic impact approach, the analysis can be structured towards the effect of cyber power as measured though its impact in order to establish the significance of cyber power, hereby creating a better understanding of what effect cyber power has on the international system. More specifically, it allows for an analysis that highlights the ability of cyber power to affect specific elements in the international arena by addressing all three pillars in the model of cyber power, resulting in a sound fundament to ultimately assess the application of middle power theory in the cyber realm though agility.[31] As Keohane noted this approach to power shifts analysis from the claim of possession of power to the actual effects it brings along. Systemic impact in that sense is reached through cooperation with other states or through international institutions.[32] The methodology section will elaborate on the ways in which systemic impact is to be incorporated in the framework.

A nuance that must be made regarding the concept of middle powers is between emerging and traditional middle powers. This distinction is important to describe as both ascertain different policy goals in IR, as will be described below. The information is important as it is an essential aspect of the body of knowledge regarding middle powers. The Netherlands and South Korea can both be classified as traditional middle powers.[33] However, as described above, South Korea has experienced a policy change which could also designate it as an emerging middle power.[34] Eduard Jordaan described middle powers as 'states that are neither great nor small in

[30] Carr, 79–80.
[31] Carr, 78–79.
[32] Keohane, 'Lilliputians' Dilemmas', 296.
[33] Oosterveld and Torossian, 'A Balancing Act: The Role of Middle Powers in Contemporary Diplomacy', 7.
[34] Melissen and Sohn, 'Leveraging Middle Power Public Diplomacy in East Asian International Relations', 2015, 3.

terms of international power, capacity and influence, and demonstrate a propensity to promote cohesion and stability in the world system.'[35] The differences between traditional and emerging middle powers can be divided into two aspects.[36] Firstly, there are a few constitutive factors that differentiate traditional from emerging middle powers. These factors are, among others, their time of emergence as middle powers and their democratic tradition. Traditional middle powers typically emerged during the cold war and have longstanding, stable social democracies whereas emerging middle powers emerged after the cold war and have relatively new and unstable democratic systems.

Moreover, several behavioural factors differentiate traditional from emerging middle powers. These differences are important to mention in this research as it demonstrates why in this case two traditional middle powers have been selected. To start off, traditional middle powers have an appeasing foreign policy focus with a global orientation whereas emerging middle powers are usually seen as reformist and focussed mainly on their own regional influence.[37] More importantly, while emerging middle powers aim to reform their region and thereby distance themselves politically and economically from weaker states in the region, the neutral brokering position for traditional middle powers allows for the mediation of international conflicts. This neutrality stems from fear of being subject to dominating hegemonic influence. Therefore, they choose to specialise in policy niches in order to establish an international identity which is clearly distant from that of the great powers.[38] For this reason, two traditional middle power states have been selected as cyber power revolves around disproportionate influence by states more powerful than the middle power in question. This notion will be discussed more elaborately in the analysis.

A final theoretical notion regarding the concept of middle powers should be dedicated to way in which middle powers seek to underline their middle power status. In order to influence international decision making through soft power politics, middle powers exercise niche diplomacy to maximise influence in these policy areas. As they have limited resources, focus is put on carefully selected policy areas. Behringer notes that niche issues are usually those that 'great powers have largely overlooked'.[39] However, the issue of human security was first put on the international agenda by middle power Canada.[40] The same trend is visible in cyber power

[35] Jordaan, 'The Concept of a Middle Power in International Relations', 165.
[36] Jordaan, 168.
[37] Jordaan, 176.
[38] Jordaan, 177.
[39] Behringer, 'The Dynamics of Middlepowermanship', 21.
[40] Behringer, 14.

where an increasing number of middle powers actively influence the current international debate. As was the case with the human security are as described by Behringer, middle powers have the capacity to influence the (cyber) security field when executing an effective public diplomacy strategy.[41] This notion is in line with the notion that security issues are always seen as vital issues and, in this sense, cyber power is not overlooked by great power states.

In conclusion, middle power theory does not funnel towards a conclusive definition. For this project a combination of a state's position, behaviour and identity will demonstrate its middlepowermanship. This framework will be applied to the Netherlands and South Korea in the methodology section to determine their middle power position. Afterwards, the next chapter will demonstrate how cyber power will be measured in both states in order to eventually answer the question how agility relating to cyber power is influenced by their middle power status.

Concepts and definitions

Cyber security

Next to middle power theory, it is of adamant important to clarify the concept of cyber security. Cyber is a term with a scope that entails all activities and objects relating to the internet. With the emergence of the internet and later on cyberspace, cyber hardware became part of states' critical infrastructure while largely being in private ownership.[42] It is interesting that for such an important aspect of state and human security there is no globally adopted definition. In relation to state security, Chourchi specifies cyber security as being the ability of a state to protect itself and its institutions against threats, espionage, sabotage, crime and other destructive e-interactions.[43] On a more general level, Solms and Niekerk define cyber security as not just the protection of cyberspace, according to them it also includes the protection of all functionaries in cyberspace and those that can be reached via cyberspace.[44] In this term, it is seen as a broader phenomenon making it even more difficult for governments to ascertain a high level of protection.

[41] Eytan Gilboa, 'The Public Diplomacy of Middle Powers: Navigating the Middle', 26.
[42] Shore, Du, and Zeadally, 'A Public-Private Partnership Model for National Cybersecurity'. 169.
[43] Nazli Choucri, *Cyberpolitics in International Relations*, 39.
[44] von Solms and van Niekerk, 'From Information Security to Cyber Security', 101.

Cyber space

An authoritative definition of what cyberspace entails was drafted by the Pentagon in 2008. The team of experts working for the USA government defined cyberspace as: 'the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.'.[45] Another definition by Lior Tabansky is: 'cyberspace is composed of all the computerized networks in the world, as well as all end points that are connected to the networks and are controlled through commands that pass through these networks'.[46] In this sense, cyberspace consists of three layers. First the physical layer of infrastructure, storage devices, processors, cables transmitters et cetera, then software, which consists of various instructions which were programmes by humans and the final layer of cyberspace is the data held by machines which they use to create information.[47] Most computers networks are connecter to the internet. However, for this research it is most relevant to focus on the computer networks which are not. These networks are used to fabricate cyber weapons. In juxtaposition to traditional weapons, which are focussed on kinetic damage, cyber weapons mainly consist of software and can be divided into three groups. Offensive weapons or capabilities, mainly malware such as viruses, worms, Trojan horses et cetera and DDoS attacks. Then there are so-called dual use tools such as vulnerability scans, network monitoring, encryption and the camouflage of content and finally there are defensive capabilities such as firewalls and disaster recovery systems.[48]

To conclude, cyberspace is a wide concept encompassing all hard- and software related to communication through networks. In terms of cyber weapons, states can develop their offensive or defensive capabilities in order to respond to possible new threats from other state or non-state actors.

Cyber power

The subject of analysis for this project will be on international cyber power in middle power states. What constitutes power in cyberspace is a controversial topic. The definition of cyber

[45] Singer and Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, 13.
[46] Tabansky, 'Basic Concepts in Cyber Warfare', 77.
[47] Sliwinski, 'Moving beyond the European Union's Weakness as a Cyber-Security Agent', 2.
[48] Tabansky, 'Basic Concepts in Cyber Warfare', 79–80.

power that will be used in this project is 'the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power'.[49] This definition by Kramer and Wentz allows for an elaborate analysis on the issue mainly because it is allows for the inclusion of all factors which are relevant to the topic of this research regarding offensive and defensive capabilities and soft power initiatives relating to diplomacy as agreed to be one of the instruments of power that state actors possess. It is important to note hereby, as Nye describes, that cyber power is a means to produce the preferred outcomes within cyberspace or in another domain outside of cyber space.[50]

Agility

As notes by Cooper, both domestic and international forces have an important impact on the international prestige of middle power states. Hereby, middle power states have become 'squeezed' by different economic, diplomatic and cultural forces.[51] In addition, the space that was formerly occupied by traditional middle powers is becoming more occupied with emerging middle powers aspiring reach the same goals.[52] In line with Cooper, for this project agility will entail of the manoeuvring space that middle powers have to set out and follow their own policy, while operating under a condition of relative and absolute safety stemming from their relations with smaller states and in the case of cyber power more importantly, with great powers that possess more means to carry out offensive and defensive cyber-attacks. In this manner, when a middle power state is highly agile, it means that their niche focus on cyber in this case yield them a better diplomatic position in the international arena.

[49] Kramer, Starr, and Wentz, *Cyberpower and National Security*, 38.
[50] Nye, *Cyber Power*, 4.
[51] Andrew F. Cooper, 'Middle Powers: Squeezed Out of Adaptive', 29.
[52] Andrew F. Cooper, 29.

Methodology and research design

This chapter will elaborate on the methodological challenges related to this research. It will give clear indications and justifications in order to make the final conclusion flow logically from the analysis. In order to achieve this, the research method and case selection will be defended and the most relevant concepts will be operationalised and the limitations of this project will be discussed.

The model of cyber power

In order to establish a structured answer to the question of how cyber power constitutes the international focus, or niche, of middle powers The Netherlands and South Korea a framework will be used which is based on the findings of David Betz and Tim Steven in their paper 'Cyberspace and the State: Toward a Strategy for Cyber-Power'.[53]

The application of the four dimensions model of cyber power will form the framework to answer the research question by addressing four categories that constitute cyber power. The four dimensions model for cyber-power was established by Betz and Stevens. The following section will outline the model and elaborate on the four different dimensions, the limitations of the model and how it will be applied to the respective case studies.[54] According to Betz and Stevens, cyber power is merely the manifestation of power in cyberspace which has different characteristics and forms.[55] They structured the model in such a way as to address a multitude of actors ranging from state to non-state actors and civil society. In order to retain focus of analysis, the model will be limited to state actors unless the inclusion of other actors in the analysis is necessary as to analyse a state actor in a complementary manner. In the following section the four types of power will be defined. In line of this, their model attempts to answer the question what constitutes state cyber power. They distinguish types of power, respectively those are; compulsory, institutional, structural and productive power which will be defined in order to compare the two cases.

The first type of power addressed in the model is Compulsory Cyber Power. It entails the use of direct coercion by an actor in cyberspace that can take place between state actors or vis-à-

[53] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*.
[54] David Betz and Tim Stevens, 45–53.
[55] David Betz and Tim Stevens, 44.

vis non-state actors. The aim of compulsory cyber power is mostly to affect electronic equipment or machinery with the result of changing the behaviour of the other actor. In addition, by deploying non-material resources such as a distributed denial-of-service attack (DDoS) in with the aim of affecting the behaviour of others in a direct way. This includes the threat of military measures of economic sanctioning according to Betz and Stevens.[56]

What is more, the second component of the model is Institutional Cyber Power. This indirect control of an actor in cyberspace is done primarily via mediation though formal and informal institutions. It is important to note that the institutions do not operate under the control of a specific state as this would amount to the previously mentioned compulsory cyber power. In essence, institutional cyber power is present when an actor is enabled to influence the way in which institutions work by steering the actions and conditions of existence of other actors. Concretely, this means that state resources are used in order to influence the setting of norms and standards of institutions or to influence the opinion of foreign audiences' trough media institutions. This does not limit itself to hard power measures. Moreover, soft power can be used to initiate cyber deterrence trough international institutions by influencing normative change in cyberspace.[57]

The third dimension described in the model by Betz and Stevens is Structural Cyber Power. This category aims elaborate on how cyberspace maintains existing international structures in which the actors are located. These structures either enable or prevent measures that an actor may want to take vis-à-vis other actors in the same structure. It is important to delineate here that the structural cyber power dimension primarily questions whether cyberspace helps existing structural forms or if it facilitates the initialisation of new structures. Herein, cyberspace does not change the international order per se, however it is important to question whether it enables the creation of new ones or if it merely sustains existing structures. Elements of cyberspace such as the internet did for example bring about the Arab Spring in 2011. In the structure of the affected states, cyberspace empowered those that without it would stand powerless against the existing structure, while they remained unempowered relative to the economic or military system for example. The Arab spring however is a profound example of how the internet as a tool of cyberspace that caused governments to fall. Structural power can help maintain the status quo or disrupt it.[58]

[56] David Betz and Tim Stevens, 45–46.
[57] David Betz and Tim Stevens, 47–48.
[58] David Betz and Tim Stevens, 48–50.

Lastly, Productive Cyber Power is allocated as the final form of cyber power in the model of Betz and Stevens. Productive cyber power constitutes the creation of a social subject's trough discourse which is negotiated through cyberspace. This can be done through media, broadcasting services and through the internet itself. For the area of public diplomacy in particular, productive cyber power is vital as through it discourse can be formed to the advantage of the actor. The most pressing example is an influencing mechanism to construct who are the threat actors in cyberspace. In addition, productive power in the international arena is mainly evident trough the advancement of new or existing narratives on world politics. From a state perspective this is mainly done by means of soft power.[59]

As Betz and Stevens described, cyber power does not display itself solely in one of the categories as described above. In every instance there is some overlap.[60] An interplay of related factors results in what we perceive as power. This means that cyber power is a diverse concept of which not all elements are necessarily present continuously. All different perceptions of power combined constitutes what one can perceive as cyber power.

To serve the aim of this research, the third category of, structural cyber power will not be part of the analysis as it does not serve the purpose of this research as it primarily focusses on how the cyber realm empower any structure in a state to use cyber in their advantage. This micro level analysis does not serve the purpose of this research, which is to add to middle power theory as it analyses aspects that stand too far from state-level analysis, especially taking into consideration the scope of this research project. The adapted model can be found in figure 2.

[59] David Betz and Tim Stevens, 51–52.
[60] David Betz and Tim Stevens, 52.

Cyber power	Definition	Indicators
Compulsory	- Direct coercion by an actor in cyberspace	- Direct malicious cyber-attacks that change the behaviour of the receiving state.
Institutional	- The issuing of indirect control of an actor in cyberspace though formal and informal institutions.	- Initiating proposals in international institutions and conferences - Setting norms and standards through public diplomacy and brokering.
Productive	- The creation of a social subject trough discourse, regarding the cyber realm. - Advancement of one's own interests' trough the framing of other states.	- The construction of designated threat actors in cyber space, mainly through soft power.

Figure 2: Dimensions of cyber power.[61]

Systemic impact approach

As mentioned in the theoretical framework, systemic impact is a way to assess the effectiveness of middle powers. By applying this approach, middlepowermanship can be established through the outcome instead of the intention for action. Carr hereby defines a systemic impact approach to middle power as 'states that can protect their core interests and initiate or lead a change in a specific aspect of the existing international order'.[62] Concretely, this definition can establish systemic impact through the cyber power model by assessing two main elements. Firstly, though the protection of core interests through high retaliation costs in a non-traditional form and secondly through the ability to alter specific elements in their international system through institutions, treaties and formalised structures, in other words, diplomatic effort. These two pillars will eventually be used to determine how cyber power as a niche has defined the agility of the Netherlands and South Korea.

[61] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power.*
[62] Carr, 'Is Australia a Middle Power?', 79.

	Definition	Indicators
Element 1	The state possesses the capacity to protect their core interests by the ability to induce high retaliation costs in the event of an attack on its core interests.[63]	The extent and amount to which cyber related incident occur, are deterred or effectively mitigated.
Element 2	The state possesses the ability to alter specific elements of the international order through institutions, treaties and formalised structures. [64]	The imposition of norms or balances of power through diplomatic channels.

Figure 3: Systemic-impact analysis

Research method

When following Rohlfing, a case study entails an empirical study that 'is an instance of a population of similar empirical phenomena'.[65] In line with this definition, this thesis will determine whether increasing efforts by middle power states will lead to an increase or decreases in cyber power. Moreover, the population of interests in this case can be divided into three empirical categories that together constitute the extent to which cyber power increases or decreases, as can be seen in figure 2.[66]

In order to empirically assess agility in middle power states, a case study research design is the most suitable option of several reasons. Primarily, due to the research goal and the scope of the master thesis project, in-depth qualitative research will be conducted. In addition, two interviews will be conducted with experts on the topic to further substantiate the evidence found. An interview was conducted with Sico van der Meer, a research fellow at the Clingendael, the Netherlands Institute for International Relations, who is specialised, among other subjects, in cyber security from a strategic policy perspective. In this capacity questions have been asked regarding the methodology of this research and policy related topics regarding both the Netherlands and South Korea.

The cases that are researched in this paper have to meet all criteria as set in the scope conditions. Herein, the states the Netherlands and South Korea will be used. The scope conditions for selecting these states for the cross-case comparison are that both had to meet the criteria of middle power state, also both states have to specialise, or create a niche, in cyber security

[63] Carr, 79–80.
[64] Carr, 80.
[65] Ingo Rohlfing, *Case Studies and Causal Inference: An Integrative Framework*, 24.
[66] Ingo Rohlfing, 24.

initiatives in soft and hard power, with these conditions the two cases are carefully controlled for in order to establish a causal relationship where the middle power status causes an increase or decrease in cyber power.[67]

The selection of a most-likely case study design stems from the starting point of middle power theory, this criterion has determined why the Netherlands and South Korea are most representative of the population under scrutiny. Both cases exhibit a high probability of confirming the hypothesis, which is that middle powers will become decreasingly agile due to their limit in capacity and resources despite of their focus on cyber power.[68] Because of the fact that the cases are selected in a critical manner, it is the aim of this thesis to make generalisation on the applicability of middle power theory relating to the cyber realm.

Statements on the basis of a dual case study are beneficial when it is carefully argumentized what the limitations of the findings are. In addition, the three categories or factors leading to cyber power provide a clear structure for the analysis.[69]

Case selection and sources

The following section will elaborate on how the Netherlands and South Korea both qualify as an established middle power as was said in the theoretical framework. In order achieve this, figure one will be used to determine middlepowermanship. Before doing this, it is important to establish the added value of having exactly two cases. The reasoning behind this choice is twofold.

First, both middle powers operate from a complex geopolitical context that make them unique while they both have the roughly same diplomatic ambitions regarding cyber security. While making generalisations based on a dual case study remains impossible with regards so all middle power states, the two proposed cases allow the reader to see the regional diversity between the East-Asian developed states and their European counterparts. The Netherlands is encapsulated into the European Union (EU), and while security policy primarily remains at the discretion of the individual member states, the European context is relevant to cyber security policy in the area of European cooperation and policy areas such as privacy and data-protection.[70] Second, South Korea is especially relevant for its security situation with the threat of Pyongyang's nuclear arsenal. Despite recent efforts by USA President Donald Trump, the

[67] Ingo Rohlfing, 26.
[68] Ingo Rohlfing, 84.
[69] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*.
[70] 'European Union Directive 95/46/EC'.

two states remain stuck in a long-term ceasefire position. The Korean is one of the causes for South Koreas focus on cyber security and it considers with ambitions to establish South Korea as a middle power in multiple policy areas besides cyber security. Socioeconomic initiatives hosted by Seoul have primarily focussed on Northeast-Asia and have only recently shifted attention to the entire international community.[71] As such, the combination of the two cases present a comprehensive overview of how cyber security diplomacy effects middle power states globally, taking in mind the limited scope and length of a master thesis.

Figure one sets out the criteria for middlepowermanship, comprising theoretical underpinnings and research conducted by the Clingendael Institute for International Relations in the publication 'A Balancing Act: The Role of Middle Powers in Contemporary Diplomacy'.[72] Regarding this specific research model, it is important to note that it is a purely quantitative method. One may argue that this does not suffice when aiming to establish middlepowermanship as the term is broader and should also be approached from a qualitative starting point. However, as the further research depends on the measurement of a degree of power, which is essentially subjective as it is established in relation to other actors, it is useful to start from a quantitatively determined foundation regarding the case selection, hence the establishment of middlepowermanship.

The Clingendael model will be applied to both the Netherlands and South Korea in order to determine their middlepowermanship by positioning them between the great powers and smaller states. As with middle powers, there are multiple ways in order to determine who are the current great powers. One of the ways defining great powers is by denoting those states that possess at least five percent of the world's population, economy or military power or those that are member of the United Nations Security Council (UNSC).[73] Currently, that means that the USA, China, Russia, the United Kingdom (UK), France, Japan, and Germany and India are the eight current great power states.

With the great powers in mind, the positional approach established middlepowermanship by means of quantifiable factors, most importantly differentiating between middle powers and small states as the great powers have been established already. The Clingendael Institute made such a differentiating by assigning grade points to criterion relating to GDP, population and

[71] Lee, 'New Approach of South Korea's Middle Power Diplomacy: Focusing on Global Agenda Setting', 44.
[72] Oosterveld and Torossian, 'A Balancing Act: The Role of Middle Powers in Contemporary Diplomacy'.
[73] 'A Balancing Act | Strategic Monitor 2018-2019'.

military spending where both for the positional approach The Netherlands and South Korea positioned themselves among the first fifty states below the eight great powers.[74]

The behavioural approach to middlepowermanship focusses on how middle powers act on the international stage and guide their diplomacy. In the research conducted by Clingendael, this was operationalised by comparing the size a state's diplomatic network and the amount of times it had been member of the United Nations Human Rights Council (UNHCR) or UNSC. Clingendael determined that in order for a diplomatic network to be an indicator of middlepowermanship, the state should have at least fifty embassies or consulates. The membership of the UNHCR or UNSC signalling good international citizenship should have occurred at least once. Both the Netherlands and South Korea meet the criteria of thsee behavioural approach to middlepowermanship with respectively 111 embassies and 299 consulates for the Netherlands and 119 embassies and 161 consulates for South Korea in 2011.[75,76]

Lastly regarding the identity approach highlights the actual commitment and investment that potential middle powers have towards upholding a reliable and strong image in international affairs. The Clingendael institute used two factors to distinguish between established and emerging middle powers. They assessed the contribution to global development through financial support of the UN Development Program (UNDP) between 2013 and 2017 with a minimum contribution of 0.1 percent of the total and secondly, it was assessed to what extent states were committed to upholding civil and political rights nationally through the Freedom House Index (FHI) in order to compare foreign policy with the internal situation. Both the Netherlands and South Korea meet both criteria, having contributed more than 0.1% of the total UNDP budget between 2013-2017 and being ranked as 'free' in the FHI.[77] By meeting these criteria both the Netherlands and South Korea qualify as established middle power states for the purpose of this research.

In line with Robert Cox, an assessment of middlepowermanship is heavily driven by context.[78] Besides the reasons as listed in the introduction regarding the externalities which motivated The Netherlands and South Korea to have interests in the cyber debate, the specific selection of both cases will contribute to the final assessment of middle power theory in the cyber niche. When he analysed the context of Japan's middle power status, Cox stated relating to context, 'non-

[74] 'A Balancing Act | Strategic Monitor 2018-2019'.
[75] 'Netherlands - Embassies and Consulates'.
[76] 'The Republic of Korea - Embassies and Consulates'.
[77] Oosterveld and Torossian, 'A Balancing Act: The Role of Middle Powers in Contemporary Diplomacy'.
[78] Cox, 'Middlepowermanship, Japan, and Future World Order', 825.

state forces such as international institutions play a fundamental role in the middle power debate.[79] In this project, these factors, in combination with the different approaches to middlepowermanship discussed earlier substantiate the case selection to include The Netherlands and South Korea.

As was mentioned in the introduction of this thesis, The Netherlands and South Korea both have a focus on multilateralism in their foreign policy. It is in both their interests to propagate a world order where liberal institutionalism overrules a unilateral or bilateral situation.[80] In this sense both state share the same core interest. The following section will set out how the two cases are similar and how they differ from each other in multiple ways.

In this line of reasoning, for the Netherlands, it is encapsulated in the EU' legislative structure which in forms is indirect and supranational legislation a practical and functional policies are decided in Brussels through regulations and directives. In terms of cyber security, the European Parliament adopted the Directive on security of Network and Information Systems (NIS Directive) which was to be fully implemented in November 2018.[81] The NIS Directive hereby is an important indicator of the European context in which the Netherlands operates as it has implications for its national cyber security policies.

South Korea, in turn, operates in a notably different context. This is important as it underscores the added value of having two cases instead of having only one case. While South Korea has a comprehensive free trade agreement with the Association of Southeast Asian Nations (ASEAN), the state is not a member of any such regional multilateral institution as is the case with the Netherlands.[82] While MIKTA, which was launched in 2013 and other initiatives strive for being comprehensive multilateral institutions, they are still in no manner comparable to an EU context. In terms of cyber regulations, South Korea hereby acts in a different setting than the Netherlands being less influence by a multilateral structure such as the EU.

Finally, what makes the analysis of these two cases interesting is the geostrategic difference between the cases Inter-Korean relations determine for a large part how South Korean cyber policy can develop itself as a niche in their foreign policy.[83] Long-term South Korean aspirations of an open and secure cyber environment are thwarted by its security situation. How

[79] Cox, 834–35.
[80] Sico van der Meer, Cyber power in The Netherlands and South Korea.
[81] European Commission, 'The Directive on Security of Network and Information Systems (NIS Directive)'.
[82] 'ASEAN - Republic of Korea Free Trade Area'.
[83] Sico van der Meer, Cyber power in The Netherlands and South Korea.

does this affect its agility in comparison to a middle power in a more stable condition such as the Netherlands? [84,85]

In terms of the use of sources, this research project will mainly depend on policy documents, in-depth literature on middle power theory and interviews. All of the above will help to substantiate the argument and in the end shed light on middle power theory with regards to cyber security. As a starting point, the national cyber security policies of both states will be used as a fundament and will be discussed in light of the three categories of cyber power. In addition, primary documents relating to relevant diplomatic efforts such as conferences and international initiatives will be collected to serve as indicators for cyber power in The Netherlands and South Korea. Finally, academic literature which is available concerning cyber power and relating incidents or attacks will serve to get an elaborate overview of the cyber position of both states. In the analysis part, literature relating to middle power theory as described in the methodology part will be utilised to connect cyber to the theory. Taken in unison, interviews, national cyber policy documents, reports and academic literature helps to answer the research question as it creates an image which is as comprehensive as possible in order to make tentative generalisations regarding middle power theory in the cyber realm.

Relevance and gap in knowledge

Currently, there is no authoritative academic work specifying what constitutes a middle power, there are multiple definitions. For this reason, authors devote attention to their application of the term in their specific context in mind.[86] As Robertson notes, the term middle power revolves not so much around its meaning and more about the elements of influence, persuasion and coercion that it entails. In other words, it is ultimately linked to the rhetoric behind the expression of state power in its traditional sense.[87]

From an academic point of view, middle power theory has thus far been used as a tool to analyse states in relation to the socioeconomic development of states. Australia and Canada have been used as a primary example of middle power by academics.[88,89] Policy makers designating their state as a middle power have mostly used the concept to advance the interests of their state in

[84] Sico van der Meer.
[85] Melissen and Sohn, 'Leveraging Middle Power Public Diplomacy in East Asian International Relations', 24 November 2015, 3–4.
[86] Robertson, 'Middle-Power Definitions', 359.
[87] Robertson, 355–56.
[88] Carr, 'Is Australia a Middle Power?'
[89] Ravenhill, 'Cycles of Middle Power Activism'.

multilateral fora revolving around socioeconomic themes or to demonstrate their expertise in these areas to the international community.

Military interests have not been advanced through applying a middle power lens in this sense as middle power states were specifically presumed to advance their interest through different channels not relating to hard power, mainly because of their lack in size or material capacity. This thesis connects middle power theory to the security realm, increasing the relevancy of middle power theory for policy makers and academics.

To elaborate, the development of cyberspace has given way for a new range of security related aspects that had not yet surfaced before. Among others, complexities in terms of attribution, deterrence and rapid evolvement of capabilities of cyber-attacks underscore the volatile way in which the cyber domain relates to security.[90] More importantly, the correlation between cyber-attacks and material resources is not set in stone. The damage inflicted via cyberwarfare is less directly linked to the amount of manpower and resources involved.[91] **Following this line of reasoning, cyber is the first domain related to security in which the application of middle power theory could enhance a state's level of security.** The creation of a cyber niche will shed light on the area's in which the state is more or less prone to cyber-attacks, herein increase its ability to deter future attacks and in this sense increase security.

From an academic point of view, the relevance of this project thus stem from the fact that it will assess how middle power theory interacts with the cyber realm. As stated above, no such study has yet been conducted. The systemic impact analyses to be conducted on the Netherlands and South Korea hereby connect middle power theory and the cyber domain with the aim of delivering insights in the academic relevancy of middle power theory on the cyber domain. In addition, cyber security has been subject to more technological changes than other domains.[92] While middle power theory has been applied to other field such as human security, cyber power has not been subject to a middle power analysis yet. [93] Therefore, in light of the ample research that has been done in the field of cyber power in middle power states, this thesis provides academics and policy makers with a foundation on how middle power states could use cyber to either enhance their security or as a way of advancing their interest vis-à-vis other state actors using public diplomacy.

[90] Sico van der Meer, Cyber power in The Netherlands and South Korea.
[91] Nye, *Cyber Power*, 4.
[92] Nye, *Cyber Power*, 3–4.
[93] Behringer, 'Middle Power Leadership on the Human Security Agenda'.

In sum, this thesis will connect the available literature on middle power theory to the cyber realm. The cases to be examined will then serve as examples of how to further incorporate the cyber domain in middle power literature and therefore use it to advance the interests of the states it is applied to by means of empirical research.

Caveats to this research

The limitations to this research have multiple facets. Firstly, power is a relational concept as it is defined vis-à-vis another actor. In addition, it is multidimensional as certain elements of power can increase while others decrease at the same moment.[94] The model by Betz and Stevens analyse three dimensions of power. Those three elements all influence the degree of power in an independent manner and at the same time they intertwine. Soft power initiatives in this sense can contribute to an increase in offensive capabilities, thus interacting with compulsory and institutional cyber power. Accordingly, where to attribute these forms of power t o and to wat extent in essence remains open to some degree to how the different elements of power are perceived and interpreted.[95]

Moreover, when conducting research regarding cyber security, protection of critical infrastructure and military strategies, a majority of documents contain classified information and thus are not generally available. Therefore, some aspects of this thesis have been reached using multiple secondary sources in order be as close as possible to the primary information sources. For the South Korean case, an additional problem was the language barrier, reducing the available material further. This has been solved by specifically focussing in South Korea during the background research for this thesis and asking specific questions during the interview.

Lastly, due to the scope of this project, a limited number of cases have been used with the aim of shedding light on middle power theory in the cyber domain. Two cases are a limited number when attempting to make statements on the general applicability of IR theory. Hence, the aim is to make suggestions based on the finings while being aware that middle power theory is an a broadly scoped subject which allows for multiple ways of analysis, predictability and interpretability.

[94] Baldwin, *Power and International Relations, A Conceptual Approach*, 49–51.
[95] Eytan Gilboa, 'The Public Diplomacy of Middle Powers: Navigating the Middle', 22–23.

Analysis

Both the Netherlands and South Korea are among the most connected states in the world, cyber power is for both states of exceptionally important for both the economic sector and national security, propelled by the relatively low costs and risks for the perpetrators of cyber-criminal acts.[96][97] In this sense the coasts for deflecting a cyberattack are profoundly higher than the costs of executing it.[98] The upcoming part of this thesis will constitute the establishment and analysis of cyber power in respectively The Netherlands and South Korea. As elaborated before this will be done by using the three indicators of the cyber power model after which systemic impact will be established in order to determine agility. These conclusions will hence be used in order to shed new light on middle power theory and its implications on the cyber realm.

Cyber power in the Netherlands

Introduction

In the Netherlands, foreign policy has largely been dictated by the belief that it is in the interest of the Dutch state to promote multilateralism as much as possible. Due to its size and resources, the hard power deficit and international embeddedness makes a comparable orientation of openness and inclusivity a logical next step in the cyber domain.[99] In addition to the advancement of its own interests, for the Netherlands it is an excellent opportunity to demonstrate its diplomatic capabilities in international agenda setting and mediation on relatively new policy area. In order to analyse the eventual agility of the Netherlands, its national and international cyber structure will be elaborated upon after which the model by Betz and Stevens will be used in order to establish agility.

The first authoritative document analysing the current status of cyber within governmental policy was issued under the auspices of the Ministry of Justice and Security. By an organ called GOVCERT, the former Cyber Security Emergency Response Team (CERT) of the Dutch government in 2011.[100] This document, the Cyber Security Assessment Netherlands (CSAN) is

[96] Ministerie van Buitenlandse Zaken, 'Digitaal Bruggen Slaan: Internationale Cyberstrategie Naar Een Geïntegreerd Internationaal Cyberbeleid', 2.
[97] Ju Yong-Wan, 'Survey on the Internet Usage 2017'.
[98] Ministerie van Buitenlandse Zaken, 'Digitaal Bruggen Slaan: Internationale Cyberstrategie Naar Een Geïntegreerd Internationaal Cyberbeleid', 4.
[99] Sico van der Meer, Cyber power in The Netherlands and South Korea.
[100] Ministerie van Justitie en Veiligheid, 'Cybersecurity Beeld Nederland 1 December 2011'.

published nowadays by the National Coordinator for Security and Counterterrorism which falls under the Ministry of Justice and Security. The CSAN's offer an actual image of the cyber security situation as it is in the Netherlands. Input is gathered by among others the Cyber Security Council, which is an organ of authoritative advisors from both the public and the private sector and the General as well as Military Intelligence and Security Service of the Netherlands (AIVD, MIVD).

The CSAN can be considered authoritative and reliable sources as each annual publication has been endorsed by the Cyber Security Council (CSC). The CSC is an advisory body, initiated by the minister of Justice and Security in 2011.[101] The council comprises high-level figures from the Dutch public and private sector as well as academia. The endorsement of the CSAN's by the CSC implies a high level of cooperation and transparency among the different sectors. In addition, it ensures that on a national level, cyber policy reviewed and adjusted with the most recent information available.

Thus, in the Netherlands, the governmental cyber blueprint is relatively clear. Dutch cyber policy is strongly embedded in different organs government falling under the Ministries of Foreign Affairs, Justice and Security and Defence, each ministry publishes elaborate documents which are updated on an almost yearly basis. It is important to highlight the structure of both the national and the international cyber policy in order to come to a conclusion on cyber power. Both aspects will be briefly discussed accordingly. All Dutch national and international cyber policy is based on two core documents. The Ministry of Foreign Affairs has published the Integrated Foreign and Security Strategy 2018-2022 (IFSS) and the Ministry of Justice and Security outlined its cyber objectives in the Dutch Cyber Security Agenda 2018 (DCSA), which is published annually. The documents discussed below all fall under either of these overarching documents as there are either a practical elaboration of policies or assessments of the cyber situation. In sum, the Dutch government was early to recognise the importance of an elaborate framework to integrate cyber security measures on a governmental level in order to ensure a smooth transition into the digital era.

While the ministry of Justice and Security is responsible for national cyber policy, the Dutch ministry of Defence outlines the national and international cyber policy in the Defence Cyber Strategy (DSC), which was first published in 2012.[102] In the analysis, called 'Investing in Digital Strike Power for The Netherlands', will constitute the part on hard power capabilities

[101] Ministerie van Justitie en Veiligheid, 'Cyber Security Raad'.
[102] Ministerie van Defensie, 'Defensie Cyber Strategie 2018: Investeren in Digitale Slagkracht Voor Nederland', 5.

for the Netherlands. Finally, the Ministry of Foreign Affairs has produced a complementary document next to the IFSS. This International Cyber Strategy (ICS) outlining international threats, interests and the Dutch response to these developments in the international arena. The next section will start by addressing the first part of the analysis; compulsory cyber power in The Netherlands.

Internationally, the Netherlands ranked 12th on the Global Cyber Security Index (GCSI) in 2018.[103] The index, issued by the United Nations International Telecommunications Union (ITU) is an international indication of the commitment that the member states have regarding cyber security on a national, regional and international level.[104] The position of the Netherlands on this list shows the initial willingness of the Dutch government to actively participate in capacity building in the international cyber domain.

Compulsory cyber power

As noted by Betz and Stevens, Compulsory Cyber Power entails the use of direct coercion by an actor in cyberspace. Hence, it is focussed on military means and the allocation of resources, from the national budget to in these investments related to the capabilities in the cyber realm.[105] Herein it is important to note that besides the national and the United Nations context, the Netherlands allocates offensive resources to the North Atlantic Treaty Organization (NATO), hereby influencing the extent of cyber power in the Netherlands. The government agreed on a structural allocation of 20 million euros annually from the total defence budget of 8.687 million euros in 2021. This does not seem a lot, however, in 2018 no funds were allocated to cyber capacity building yet.[106] Even if the investment in 2021 only comprises approximately 0.23% of the annual Defence budget, it is a net increase of 20 million in comparison to last year. The allocation has the aim of supporting current cyber operations for longer periods of time and the execution of new offensive or defensive operations in the future.[107]

More specifically the investments are used to ensure the security of the IT and weapon systems, including their digital resistance.[108] This has been outlined as a key objective by the ministry of defence. In addition, improving deterrence and disruption techniques on incoming attacks

[103] 'Global Cybersecurity Index (GCI) 2018', 64.
[104] 'Global Cybersecurity Index (GCI) 2018', 7.
[105] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, 45–46.
[106] Ministerie van Defensie, '2018 Defence White Paper: Investing in Our People, Capabilities and Visibility', 27.
[107] Ministerie van Defensie, 18.
[108] Ministerie van Defensie, 'Defensie Cyber Strategie 2018: Investeren in Digitale Slagkracht Voor Nederland', 5.

and the protection of critical infrastructure are amongst the key investment points by the ministry of defence in their 2018 strategy.[109] The DSC shows that from a governmental perspective, active investment is taking place on offensive and defensive capabilities, especially since 2018 with the allocation of new funds. Moreover 6.5 million euros will be invested annually in research and development in the area of cyber capabilities.[110] In sum, when focussing on the Dutch ministry of defence, it is evident that since the introduction of the fist DSC in 2012, awareness on the importance of investment in compulsory power has grown to a large extent. This will automatically the Dutch compulsory power in comparison to other states. Dispersed among the other ministries, 95 million euros has been invested in cyber security in general from the government budget from 2018 onwards.[111] This structural investment has thus far not prevented the Ministry of Justice and Security to highlight that over 2018 states have committed extensive economic and political espionage against the Dutch state.

In addition, this threat to national security is increasingly complex as hostile states will keep advancing their offensive capabilities.[112] Herein it is fair to say that Dutch national security is often affected relating to the cyber realm, even if The Netherlands is not the primary target. A pressing example is the NotPetya virus where Ukraine had been targeted by Russian hackers in 2017. In this ransomware attack, where money is demanded or certain systems will remain blocked, operational systems in major Ukrainian and also Dutch enterprises were attacked. Hereby the former TNT Post, the Dutch mail services experienced massive delays in their delivery service.[113]

Apart from the EU context, the Netherlands is increasing its visibility internationally in the cyber domain by becoming a known authority in the area of cyber capacity building. The Hague houses and finances the secretariat of the Global Forum on Cyber Expertise (GFCE). This international multi-stakeholder organisation is aimed at increasing cyber capacity building between the public and the private sector on a voluntary basis. Being located in centre of the Dutch legislative power, the secretariat is operated by personnel originating from the Dutch Ministry of Foreign affairs and Justice and Security. Although the GFCE is separated from the Dutch government, the secretariat does serve as an important agenda setting power in the organisation. In addition, the mandate to house the secretariat was supposed to expire four years

[109] Ministerie van Defensie, 5.
[110] Ministerie van Defensie, 15.
[111] Ministerie van Justitie en Veiligheid, 'Nederlandse Cybersecurity Agenda: Nederland Digitaal Veilig', 5.
[112] Ministerie van Justitie en Veiligheid, 7.
[113] Wouter van Noort, 'Hack kost Maersk honderden miljoenen'.

after its establishment in 2015.[114] However, this mandate has recently been renewed, underscoring the successful contributions of the Dutch professionals to international cyber capacity building and the establishment of best practices.

To conclude, it is evident that the Dutch hard power capabilities are able to withstand and deter various attacks and that considerable investments are being made in order to develop a strategic framework of response capabilities. Those include attribution, deterrence and other capabilities. Albeit these measures are ameliorating compulsory cyber power, other states are also focussing on elaboration of the same techniques.[115]

Institutional cyber power

Institutional cyber power manifests itself when the state is able to excerpt influence by the use of formal and informal institutions, mainly by norm setting and soft power. The Netherlands has an extensive history in the international arena of dictating norm setting in other areas such as the advancement of human rights.[116] Furthermore, in the digital domain, the Netherlands is aimed at the advancement or the international rule of law and human rights. Moreover, the goals set in 2018 by the ministry of justice and security advocate the spreading of norms in cyberspace and the strengthening of trust among state actors in cyber space.[117] In the context of cyberspace, the Dutch norms entail the advancement of an open, free and safe internet. In the coming years, this goal will be reached by stimulating the interpretation of and application of international law on cyberspace and the protection of telecommunication and critical infrastructure.[118]

As mentioned before, the advancement of trust is one of the important factor where the Netherlands ministry of Justice and Security hopes to increase Dutch cyber power. Recently the Global Commission on the Stability of Cyberspace has contributed to this goal and was partly founded by the Hague Centre for Strategic Studies (HCSS) in cooperation with the Dutch Ministry of Foreign Affairs.[119]

As the Netherlands is embedded in the structure of the European Union (EU), institutional cyber power is sometimes difficult to solely attribute to the Dutch state. In the EU, an example of a

[114] Global Forum on Cyber Expertise, 'Framework Document: Launch of the Global Forum on Cyber Expertise 16 April 2015', 4.
[115] Ministerie van Justitie en Veiligheid, 'Nederlandse Cybersecurity Agenda: Nederland Digitaal Veilig', 23.
[116] Ministerie van Buitenlandse Zaken, 'Mensenrechtenrapportage 2017: Actualisering Buitenlands Mensenrechtenbeleid En Resultaten'.
[117] Ministerie van Justitie en Veiligheid, 'Nederlandse Cybersecurity Agenda: Nederland Digitaal Veilig', 23.
[118] Ministerie van Justitie en Veiligheid, 23.
[119] Rijksoverheid, 'Toespraak Minister Blok over 1-Jarig Bestaan Tallinn Manual 2.0'.

European initiative to advance institutional cyber power is the current development of the EU Cyber Diplomacy Toolbox. This list of measures contains various diplomatic procedures in order to counter major attacks launched through cyberspace, so called Advanced Persistent Threats (APT). It is especially relevant as constituting to institutional cyber power as it is aimed at both state actors and non-state actors acting under its control.[120] The framework has not been implemented yet and its scope is still too broad to include effective responses to cyber threats, however, The Netherlands has served as a catalyst for the initial debate leading up to the toolbox.[121] In October 2018, The Netherlands contributed to the initiation of the Toolbox for it to be discussed by the Council of the European Union. In a paper written by the initiators of the Toolbox, Cyber Diplomacy is deemed an important tool in increasing cyber power as it contributes by 'increasing the costs of coercive cyber operations and establishing a deterrent effect'.[122] Hence, also in the European context, the Netherlands as middle power is on the forefront of institutionalising cyber norms. While the Toolbox is still on the negotiation table, the result will serve as a genuine norm setting framework for the entire Union.

Moreover, apart from the European context, the Dutch Ministry of Foreign Affairs launched the Taksforce Cyber during the Global Conference on Cyber Space in 2015. This taskforce is tasked with the representing the Dutch interests in specific goal of advancing a normative framework of cyberoperations among states.[123] This long-term project is aimed at an international environment which is set to create a stable environment where malicious actors can be detected and attacks can be attributed accordingly. Attribution process difficult in the cyber realm.[124]

On the long term, the taskforce focusses on diplomacy in order to spread global norms and values. As a middle power, institutional cyber power for the Netherlands is enhanced when there is a well-functioning rule of law in the cyber domain where predictability, stability and conflict prevention are pursued.[125] In line with this, the Netherlands initiated 'The Hague Process' where the applicability of international law is being discussed in line with the Tallinn Manual 2.0 and the importance of predictability in the cyber realm was stressed.[126] This

[120] Ivan, 'Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox', 8.
[121] Ministerie van Justitie en Veiligheid, 'Nederlandse Cybersecurity Agenda: Nederland Digitaal Veilig', 23.
[122] Countil of the European Union, 'Non-Paper: Developing a Joint EU Diplomatic Response against Coercive Cyber Operations', 2.
[123] Ministerie van Buitenlandse Zaken, 'Digitaal Bruggen Slaan: Internationale Cyberstrategie Naar Een Geïntegreerd Internationaal Cyberbeleid', 7.
[124] Jason Healey, 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks'.
[125] Ministerie van Buitenlandse Zaken, 'Digitaal Bruggen Slaan: Internationale Cyberstrategie Naar Een Geïntegreerd Internationaal Cyberbeleid', 14.
[126] Asser Institute: Center for International and European Law, 'The Tallinn Manual 2.0 and The Hague Process: From Cyber Warfare to Peacetime Regime'.

document compiled by the NATO Cooperative Cyber Defence Centre of Excellence offers the starting point of creating international norms on the cyber realm.[127]

Productive cyber power

The last pillar of cyber power, productive cyber power relates to discourse. How does the Netherlands frame other in the cyber realm and which influence mechanisms are in place to construct cooperative and threat actors in cyber space? Productive cyber in this sense also revolves around positive framing of certain actors in the field by means of soft power whereby the state expresses its belonging to a certain framework of likeminded actors.

In line with this reasoning, the Ministry of Foreign Affairs states that the Netherlands is in mostly resilient through international cooperation against disruptions to, breakdowns in and misuse of Information and Communication Technology (ICT). Although cooperation is the main focus in relation to Dutch productive cyber power, two exceptions where framing is occasionally used in order to construct a negative connotation with a certain actor is in the case of Russia or China. Most pressing examples are the aftermath of the possible Russian altering of the election process in the United States in 2016 and the current imposition of Chinese 5G infrastructure over Europe.[128] In this sense, the Netherlands is aided by a policy framing where this frame is elongated in the structure of the NATO and EU.

The Netherlands approaches productive cyber power in a multi-stakeholder manner, in a system anchored in international law and the integrity of the internet. The other side of the spectrum are states that prioritize increased autonomy for the state and a limited applicability of international law in the domain. In the middle of this spectrum are so-called *swing states* that do not have an outspoken preference. [129] The Netherlands hereby increases its productive cyber power by convincing swing states that their national interests are served when an open and inclusive internet is advocated and pursued in policy choices.

[127] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.
[128] Ministerie van Buitenlandse Zaken, 'Digitaal Bruggen Slaan: Internationale Cyberstrategie Naar Een Geïntegreerd Internationaal Cyberbeleid', 4.
[129] Ministerie van Buitenlandse Zaken, 5.

Agility – The Netherlands

In order to make the link between middle power theory and the cyber realm, agility will be demonstrated through systemic impact of, in this case, Dutch international cyber power. In the above, the strategy is expressed through its cyber power. These findings will in turn be used to determine systemic impact by using the two criteria spelled out in figure 3. In short, systemic impact is described by Carr as 'the capacity of these states to affect the international system'.[130] Hereby, the outcome is measured rather than intention in relation to offensive capacity and diplomatic ability for effecting change in the international system.[131] Hence, a certain level of predictability can be deducted eventually. These outcomes will be used in the final analysis on the effectiveness middlepowermanship in the cyber realm.

The first criteria, the ability of protecting a state's core interests in the cyber realm is in the case of the Netherlands strongly connected to its geostrategic position and its embeddedness in international structures such as the NATO, protected under article 5, and EU, where the Commission is elaborating an integral cyber strategy in 2013.[132] Taking into consideration these structures, the Netherlands is nevertheless affected by malicious attacks that pose substantial threats to the Dutch state, in particular stemming from the Chinese and Russian governments, both great power states.[133] Transparency is high in the Dutch capabilities, and elaborate documentation is available while especially from a compulsory power perspective the effectives of the first element remains relatively low while on an institutional level, the Dutch they are embedded in various structures in that sense elevated by the system they are situated in.

The second criteria, where the Dutch diplomatic network and multi-stakeholder strategy comes into place. As is visible in other policy fields, in the cyber realm the Dutch are successful in advancing their norms in cyberspace through active contribution to an open and secure cyberspace by means of public diplomacy, their active contribution to The Hague Process and for example the foundation of the GFCE, which can be deemed successful by means of its extended mandate by the international community.

In sum, it remains clear that especially regarding the second criteria, the Dutch are relatively prominent regarding the creation of an international normative framework regarding cyber

[130] Carr, 'Is Australia a Middle Power?', 71.
[131] Carr, 79.
[132] European Commission, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace'.
[133] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Jaarverslag AIVD 2018 - Jaarverslag - AIVD', 8.

regulation. However, a clear focus in the Dutch policy remains hard to be seen.[134] The risk here is that the Dutch efforts will not be attributed to them in the end, or that more resourceful states will finish the initiatives that were founded and supported from the Hague.

Agility expressed through a model of systemic impact, based on the cyber power model by Betz and Stevens revolves around the extent to which the Netherlands as a middle power is able to set out and pursue its own policy as separated from great power politics and other dynamic actors affecting the international system. From the analysis made above it stems that for the Netherlands there is a precarious balance. Its status as an expert on spreading norms of freedom an openness also applies to the cyber realm while for defence against seriously malicious attacks, it largely depends on the deterrent effect of its international embeddedness.

To conclude, it is in the interest of the Dutch to focus in the cyber realm on continuing a policy of stability, international agreements and predictability.[135] In this sense, the Korean case will shed new light on a situation where these formalised structures play a vastly less pronounced role while productive point of view, the visibility of an actual threat actor will have a different effect on agility.

Cyber Power in South Korea

Introduction

South Korea's relation with the cyber realm can be described as ambiguous. On the one hand it's tech sector ranks as the best in the world with internationally dominant brands such as Samsung, in addition has one of the fastest internet connections globally.[136] Bedsides this, the inter-Korean conflict makes South Korea one of the most seriously targeted states with regards to offensive cyber-attacks.[137] Both aspects make that cyber is a niche which South Korea must focus on in order to retain its international market position and more importantly safeguard its own security on the long term.

Primarily, it is relevant to point to the structural differences that exist between the way in which cyber policy is institutionalised between the Netherlands and South Korea. As was demonstrated in the previous case, policy regarding cyber is highly institutionalised in the

[134] Sico van der Meer, 'Medium-Sized States in International Cyber Security Policies', 4.
[135] Ministerie van Buitenlandse Zaken, 'Digitaal Bruggen Slaan: Internationale Cyberstrategie Naar Een Geïntegreerd Internationaal Cyberbeleid', 14.
[136] Sico van der Meer, Cyber power in The Netherlands and South Korea.
[137] Chanlett-Avery et al., 'North Korean Cyber Capabilities: In Brief'.

Netherlands, albeit divided over various ministries and respective sub organisations. Herein, the policy can be traced back to two primary documents, for foreign and domestic policy. The Korean cyber landscape is more fragmented and sources are available in less detail than in the previous case. Nevertheless, a conclusive image can be deducted reflecting the Korean policy in previous years, retaining the explanatory power to shed light on its cyber power.

South Korea has a had a desire to gain more influence on the world states since the start of this century. The state has demonstrated that it wants to contribute in the fields of economy, development and security. In 1996 South Korea joined the Organisation for Economic Co-operation and Development (OECD).[138] Under Lee Myung-bak, South Korea began effective middle power diplomacy.[139] In recent years is has hosted, among other events, the Nuclear Security Summit and the G20 leaders' meeting in 2010 and it currently participates actively in peacekeeping and military operations across the world, thus promoting global peace and security while spreading its norms and advancing its interests indirectly.[140] The conditions for South Korea to pursue middle power diplomacy are favourable at first sight. It is geographically located between East Asian great powers China and Japan and developing states as part of ASEAN. Furthermore, it is not capable of posing a military threat to these states while holding close strategic ties with China, Japan and the US.[141] On the other hand, South Korea is contained by the geopolitical conditions regarding North Korea.[142]

Regarding the cyber realm, South Korea is known as an "Internet Strong Nation". It is known for its innovative digital technology, one of the most connected states in the world and its cutting-edge internet speed rates. [143] The development of this network commenced with the creation of the current Korea Internet and Security Agency (KISA) in 1996 served as a catalyst for a move towards digitalisation. Since then, the issue of cyber power has been gaining traction. In 2011, the Korean government announced plans to initiate a National Cybersecurity Masterplan in response to the threats posed by North Korea.[144] The masterplan was composed by 15 government agencies. Herein, cyberspace is considered a part of the Korean national territory, hereby needing a comprehensive national defence system.[145] The National Intelligence Services (NIS) oversees the National Cybersecurity Center (NCSC). Hence, the

[138] Kim, 'Korea's Middle-Power Diplomacy in the 21st Century', 4.
[139] Kim, 5.
[140] Shim and Flamm, 'Rising South Korea', 384–85.
[141] Kim, 'Korea's Middle-Power Diplomacy in the 21st Century', 4–6.
[142] Sico van der Meer, Cyber power in The Netherlands and South Korea.
[143] Sangbae Kim, 'Policy Recommendation for Cyber Security South Korea's Middle Power Diplomacy:', 2.
[144] James Andrew Lewis, 'Advanced Experiences in Cybersecurity Policies and Practices', 36.
[145] James Andrew Lewis, 36.

NCSC is tasked with the coordination of deterring, analysing and investigating cyber security incidents. The final development regarding cyber power occurred in 2015 with the appointment of a presidential adviser regarding cybersecurity matters.[146]

As mentioned before, South Korea responsibilities relating to cyber security have been fragmented among different government organisations. Next to the NCSC, the National Cyber Threat Joint Response Team, that is composed of public, private and military bodies, works in cooperation with the NCSC when a crisis situation occurs. Herein, the coordination in times of a crisis situation is the responsibility of the Korean Computer Emergency Response Team/ Coordination Center (KnCERT/CC).[147] Lastly the Ministry of National Defence (MND) oversees the operational cyber security from a military perspective.

On an international level, KISA has been an active contributor to the drafting of the Global Cybersecurity Index (GCI) 2018.[148] In the report, Korea is ranked 3rd in the world regarding the effectiveness of its e-Government infrastructure.[149] On the global GCI scale South Korea ranks 15th. The discrepancy between the two results is striking as it signifies that although the Korean digital governmental environment is highly advanced in comparison to other states while in terms of its level of Cyber Security readiness it remains 15th place.[150] While in comparison to the global readiness this is a relatively high score, the discrepancy between the two indices remains relevant as they should go hand in hand ensuring a safe e-Government environment. All in all, especially in comparison to the Netherlands, the Korean strategy towards cyber is far less embedded, it is not integrated across all facets of government.

As with the previous case, the following three sections will structure the analysis on South Korean cyber power by applying the framework which is established by Betz and Stephens. Afterwards a conclusion of South Korean agility will be formed by means of looking at systemic impact, in which the three components of the cyber power model will be integrated.

Compulsory cyber power

Direct coercion by an actor in cyber space, is the main component of Compulsory Cyber Power in the model by Betz and Stevens, mostly expressed through the specific allocation of resources to military force and cyber capabilities. [151]

---

[146] Tae-jun Kang, 'South Korea Beefs Up Cyber Security With an Eye on North Korea'.
[147] Korea Internet and Security Agency, 'Korea Internet White Paper 2017', 90.
[148] 'Global Cybersecurity Index (GCI) 2018', 7.
[149] 'Global Cybersecurity Index (GCI) 2018', 21.
[150] 'Global Cybersecurity Index (GCI) 2018', 64.
[151] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, 45–46.

First of all, in relation to Compulsory Cyber Power, the National Cybersecurity Masterplan is updated regularly from 2011 onwards, herein a specific focus is placed on public-private cooperation and early detection of cyber-attacks.[152] Herein the main threat actor in the geostrategic playing field of South Korea is North Korea and the ongoing cease-fire situation. Because of this, the South Korean Ministry of National Defence dedicates a proportional part of its Defence White Paper 2017 to North Korea as a threat actor. Herein it is important to stress that North Korea is not the sole perpetrator of South Korean firewalls. During the Olympic Winter Games in 2018, Russian state hackers overloaded the website of the Games, hindering access to visitors. Most likely this was done in a reaction to the exclusion of Russian sportsmen to the Winter Games for the use of prohibited narcotics to boost their performance.[153]

In the cyber realm, South Korea is threatened by North Korea on a small and large-scale level. South Korean companies are mainly targeted by North Korean malware, emails with infected links or malicious content that disrupt processes on the receivers' device once opened.[154] On a large scale, two major attacks have been directed towards Seoul stemming from Pyongyang. In 2009, governmental computer networks were targeted with DDoS attacks affecting approximately 12.000 computers in South Korea and 8.000 computers abroad.[155] This is one of the earliest large-scale cyber-attacks after the attacks in Estonia in 2007. The second largest attack in 2013, attributed to North Korea distributed malware called 'DarkSeoul' which was specifically targeted to paralyse the banking sector inflicting almost 600 million euros of damage.[156] These major attacks contributed to the realisation that offensive and defensive cyber needed to be raised and professionalised in order to respond effectively to these serious cyber threats. Concretely, according to the MND, North Korea is heavily investing in cyber offensive capabilities with a unit of cyberwarfare specialist consisting of 6,800 hackers.[157] Hereafter, compulsory cyber power has increased for South Korea out of a sense of urgency. Former Minister of National Defense Han Min-koo ensured that South Korea is preparing more thoroughly for North Korean aggression.[158]

In addition to this strive of national capability building, South Korea as a middle power invests in its alliance with the United States of America (USA). The cooperation is ever growing and

[152] James Andrew Lewis, 'Advanced Experiences in Cybersecurity Policies and Practices', 37.
[153] NCSC, 'Cybersecuritybeeld Nederland 2017', 13.
[154] NCSC, 30.
[155] Mansourov, 'North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance', n.d., 13.
[156] Chanlett-Avery et al., 'North Korean Cyber Capabilities: In Brief', 8.
[157] Korea Internet and Security Agency, 'Korea Internet White Paper 2017', 17.
[158] Ministry of National Defense: Republic of Korea, '2016 Defense White Paper', 6.

in 2013 the mutual Cyber Cooperation Working Group (CCWG) was set up in order to strengthen capacity building, convening twice a year. In addition, both states are investing in infrastructure to better exchange cyber related intelligence. Finally, in 2016, a military Cyber Task Force was established in order to intensify defence cyber cooperation between the two states.[159] Recently, the relation between the USA and North Korea have been freezing, after the short seemingly rapprochement over Nuclear proliferation between President Trump and Kim Jong-un. Hence it is in the interest of both the USA and South Korea to intensify their joint effort to strengthen mutual compulsory cyber power in order to deter attacks coming from Pyongyang by proactive action and pre-emption.[160]

Institutional cyber power

South Korean former deputy minister of foreign affairs, Lee Kyung Soo highlighted the role of middlepowermanship in East Asia, especially in the setting of norms and rules for, among other areas, the cyber realm.[161] Institutional cyber power in South Korea mainly manifests itself through international conferences where norms of an open and inclusive internet are spread. The most pressing example is the annual Seoul Conference on Cyberspace where South Korea actively leads discussions in the area of cyberspace thus elaborating norm setting as a means of enhancing international prestige and advancement of their self-interests.[162]

South Korea proves to be successful in sharing its multi-stakeholder approach to cyber on various other international fora as well. Herein the state has submitted and has been an active promotor of open internet governance principles at the NETmundial meeting in Sao Paulo in Brazil in 2014.[163] As one of the most connected states on earth, it is in the interest of South Korea to spread norms of openness, accessibility and flexibility of a secure cyber realm.[164]

Furthermore, from a military perspective, the MND significantly raises institutional cyber power is the annual Seoul Defense Dialogue (SDD) where cyber security is one of the most dominant topics.[165] These conferences are attended by (vice-)ministers of defence from the Asia Pasific region, annually since 2012 in order to improve the security of the region on multiple facets. The SDD becomes increasingly institutionalised, with its scope spreading to the other

[159] Ministry of National Defense: Republic of Korea, '2016 Defense White Paper', 148–49.
[160] Ministry of National Defense: Republic of Korea, 39.
[161] Hau Boon Lai, 'Smaller Countries Can Be A Middle Power in East Asia.
[162] Korea Internet and Security Agency, 'Korea Internet White Paper 2017', 124.
[163] NETmundial, Global Stakeholder Meeting on the Future of Internet Governance.
[164] Korea Internet and Security Agency, 'Korea Internet White Paper 2017', 124.
[165] Sico van der Meer, 'Medium-Sized States in International Cyber Security Policies', 5.

continents.[166] An example of this institutionalisation is the establishment of the Cyber Working Group Meeting in 2014 where a blueprint was formed for multilateral security cooperation on cyber security.[167]

Further international norm setting is achieved through multiple initiated by KISA. The 50th Internet Corporation for Assigned Names and Numbers (ICANN) conference led to the opening of a regional office in Seoul. ICANN allocates, among other things, Internet Protocol (IP) addresses and thereby is one of the most fundamental organisations in cyberspace. In line with KISA policy, the regional office will enable South Korea to enforce influence on fundamental topics in cyberspace through direct communication with international organisations through ICANN and hereby participate in international decision-making process, hereby influencing institutional cyber power.[168]

On a final note, with an increased number of transnational cyber-attacks in 2016, KrCERT/CC demanded more international cooperation to establish an international consensus to combat those attacks. Flowing from this demand KISA put forth the Cybersecurity Alliance for Mutual Progress (CAMP). This global alliance consists of 53 international institutions, with the aim of establishing a platform to promote a secure cyberspace trough confidence-building. Since then KrCERT/CC chairs CAMP and serves as secretariat.[169] CAMP hereby ran by officials of the South Korean government ensuring that its interests are safeguarded in this way.

Productive cyber power

In South Korea, productive cyber power mainly revolves around the inter-Korean conflict. From a security and economic perspective, it is in the interest of South Korea to influence international perception of the conflict in order to gain international support. While most states confirm the status of North Korea as an international threat, it is in the interest of South Korea to continuously reinforce this subject image in order to create advantages.

In terms of influence mechanisms used by the MND, South Korea's security objectives in 2017, especially 'contributing to regional stability and world peace' bolstered national security by promoting common interests with regional neighbours to broaden the scope of security cooperation.[170]

[166] Ministry of National Defense: Republic of Korea, '2016 Defense White Paper', 165.
[167] Ministry of National Defense: Republic of Korea, 165.
[168] Korea Internet and Security Agency, 'Korea Internet White Paper 2017', 125.
[169] Kim Suck-hwan, 126.
[170] Ministry of National Defense: Republic of Korea, 41.

Moreover, the MND makes effective use of 'Asia's Paradox' where deepening economic interdependency greatly overpasses Asian security cooperation. To harmonise cooperation, the South Korean government under former president Park had aimed to set up an effective structure called the Northeast Asia Peace and Cooperation Initiative (NAPCI). This was part of her vision of *Trustpolitik* as a blueprint for the thus far missing multilateral cooperation in the Northeast Asian region, inspired by the Helsinki process in the EU. [171] NAPCI is an important factor of productive cyber power as it is specifically aimed broadening the scope of cooperation on 'controversial issues', pointing to North Korea and it offensive nuclear and cyber programmes.[172] The emphasis by the South Korean government is laid on the fact that these threats are transnational, such as the hack of Sony Pictures by North Korea in 2014 after a comedy movie mocking the North Korean president.[173] As a consequence, the negative narrative of North Korea as an threat to all states is reinforced, which is in the interest of South Korea's cyber policy.

According to Sico van der Meer, productive cyber power in South Korea cannot not be seen as an isolated area of national defence policy. Especially now that the international consensus regarding North Korea is volatile, as propelled by US President Donald Trump. While the previous two summits between Trump and North Korean Leader Kim Jong-Un have not led to a long-term rapprochement regarding North Korea's nuclear programme, it is evident that international politics had a profound effect on the productive power in South Korea as a subject of great power politics. This policy change flows through to the cyber domain, affecting international sanctions against North Korea, setting back South Korea's ability to increase its power through social discourse.[174]

Agility – South Korea

As with the previous case, agility will be assessed though systemic impact of the South Korean cyber policy. Cyber power has been analysed according to the three pillars of Betz and Stevens model of cyber power; the findings will serve as a foundation for agility trough the two elements of the systemic ability scheme. Firstly, South Korea's ability to protect its core interests through

[171] Kim, 'NAPCI and Trilateral Cooperation', 3.
[172] Ministry of National Defense: Republic of Korea, 40.
[173] Ministry of National Defense: Republic of Korea, 34.
[174] Sico van der Meer, Cyber power in The Netherlands and South Korea.

cyberspace and secondly its ability to alter the international order relating to the cyber realm, as described in figure 3.

The manoeuvring space, agility, that South Korea has to set out and follow and independent cyber policy is different from that of the Netherlands for various reasons. Coercive cyber power in South Korea specifically steered against one major threat actor. Hereby the core interest of national security in South Korea is more existential than that of most other states. While South Korea is one of the most wired states worldwide, has an effective military power and effective international diplomatic relations, retaliation against North Korea has not proven to be effective thus far for various reasons. Primarily, while the situation mainly is gauged against South Korea, deterrence is ensured by the precarious nuclear balance of power between its allies and specifically the US. Similarly, so in the cyber domain where South Korea's offensive capabilities do not overrule those of North Korea, thus also largely being dependent on the US for defence and deterrence.[175] It is safe to argue that from a cyber perspective, the threat of a North Korean attack is even greater than from a nuclear point of view, relating to the difficulty in attribution of cyber-attacks and the political costs a nuclear attack would entail.[176,177] Herein, impact proves to be difficult in the case of such fundamental threats as is less visible for the Netherlands which automatically restricts agility in a dependent defence relationship.

The second element of the model regards the international system and the extent to which South Korea in this case is able to influence the international cyber system by means of diplomacy. As demonstrated by the institutional cyber power as excreted by South Korea it is active in international institutions in order to promote its values of openness and accessibility of the internet. This is effective in the sense that the government is actively promoting these norms in for a such the establishment of the Tallinn Manual 2.0 and the annual SDD. In the cyber realm, the question of effectiveness of like initiatives remains controversial as long-term results are impossible to oversee.[178]

All in all, agility herein is expressed through the two elements of the systemic impact model. To what extent South Korea is able to dictate its independent foreign policy in the cyber domain is dictated by its geostrategic position more than that of the Netherlands. Herein it is important to note, as was visible in the GCI Index, that there is a relatively high discrepancy between South Korean internet connectivity and its level of cyber security capabilities and standards.

[175] Mansourov, 'North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance', n.d., 3.
[176] Mansourov, 3.
[177] Sico van der Meer, 'Cybersecurity Thematic Study Clingendael Strategic Monitor 2017', 11.
[178] Sico van der Meer, Cyber power in The Netherlands and South Korea.

While hosting and contributing to influential cyber security for institutions such as the SDD, the GFCE and multiple substantive cooperation initiatives with allied states, international political consensus on North Korea undermines South Koreas security in an overarching manner.[179][180]

[179] Ministry of National Defense: Republic of Korea, 155–70.
[180] The Council on Foreign Relations, 'South Korea's Difficult Path as a Middle Power in International Cyber Politics'.

Conclusion

The aim of this thesis was to add to middle power theory by focussing on two cases, The Netherlands and South Korea. The cyber realm has been taken as a niche from which to assess how it interacts with the theory by looking at systemic impact of cyber power and essentiality how this affects the states' agility. Agility herein was a concept that is newly introduced in this project to serve as a graduator on the manoeuvring space that middle powers have in their foreign policy choices. To achieve this goal, the following research question has been introduced:

How does the prioritization of cyber security policies affect the agility of The Netherlands and South Korea as middle powers in the international environment?

The conclusion will answer the research question by elaborating on the key findings in both cases, after which a final statement will be made regarding middle power theory in the cyber realm.

Cyber agility in middle power states

The Netherlands

In the Netherlands, agility in the cyber realm is expressed in a juxtaposition between its evident deficit in hard power capabilities versus the professionalism with which the Dutch government is able to effectively engage in international institutions in order to advocate an international normative framework of openness and multilateralism. However, with regards to its hard power deficit, the state remains almost entirely dependent on its international embeddedness in structures such as NATO and the EU. In addition, as Sico van der Meer has righty pointed out, the Netherlands has the tendency to apply a broad focus on a large amount of issues. Hereby it remains the question how effective this focus would be if it was narrower and more precise.[181] Thus, systemic impact herein seems considerable, regarding the second criteria, less so with the first, the ability to protect its core interests in cyberspace. With regards to overall agility it is therefore fair to say that in the structures available, the Netherlands is to a large degree agile as

[181] Sico van der Meer, Cyber power in The Netherlands and South Korea.

its structure allows it to be so. On the long term it makes it hard to say whether this will remain the case as security in the cyber realm remains an aspect that is volatile and still subject to international great power politics. On a final note regarding the Netherlands, the cyber niche as pursued by the government affects agility in the sense that it in a stable situation as it is now, it is increased. The Netherlands gains international allure with its focus on cyber, while it remains the question how this will play out on the long term. On a last critical note, would there be an urgent security situation, the Netherlands would have ample space to set out its own security policy, hereby still being reliant on international structures and great power allies.

South Korea

Security considerations leads the discussion to the second case, South Korea. Situated in a different region and with a different level of institutional embeddedness it was relevant to focus on these two cases that are different in this sense as the decision to focus on a cyber niche as a means of advancing its middle power position was less so than in the Netherlands a choice rather than a necessity. The situation on the Korean Peninsula has been propelled onto the cyber domain since its development in the 1990's. As was shown in the systemic impact analysis, for the protection of its core interests in the cyber domain, South Korea is largely dependent on two factors, it alliance with the US and international or regional dynamics regarding the conflict taking in mind China, Japan and other influential actors. Hence, agility is in this respect dependent on external factors and therefore very limited.
However, it would be too limited to address the conflict as the sole driving force behind Korean strive for enhancement of its image regarding cyber power on the international stage, as it is a domain in which South Korea clearly demonstrates its excellence regarding its highly developed tech industry which is a tool for international, diplomatic prestige.

Reflecting on middle power theory, in light of agility in the cyber realm

This thesis project aimed to answer the question how the prioritisation of cyber security policy has affected the agility of the Netherlands and South Korea as middle powers in the international environment. From a theoretical foundation two cases have been studies following a model of cyber power, after which agility has been determined through systemic impact. The two cases offered insight on how conditioning influences agility on different levels of the

geostrategic spectrum, resources and embeddedness in international structures. Taking the findings in mind the following section will reflect on middle power theory when specifically applied to the cyber realm, a relatively new area that it had not been applied to before.

As was said in the beginning of this thesis, middle power theory is not set in stone. It has proven to be a useful policy tool to determine the foreign policy direction in multiple states.[182,183]

This thesis has also shown that the cyber domain in this sense is essentially different. Middle power theory herein has been linked to the cyber realm with the introduction of the concept of agility, placing it in the larger debate on middle power theory among IR scholars. The following reflections regarding middle power theory in relation to agility and cyber power are fundamental for the purpose of this research and hence would be suitable for further research as the subject is under-researched.

Primarily it is important to note that cyber security is a transboundary issue that cannot be isolated to one specific policy area. It interacts and in this sense overflow in almost all contemporary forms of communication. In general, middle power states can opt to initiate and support a multiplicity of proposals in the cyber domain. As telling as it is to understate middle power status, it remains the question whether the capacity deficit and resources in the Netherlands, South Korea and in this line of reasoning, other middle power states, allow for such a broad focus due to the borderless character of the cyber domain.

Another reflection revolves around strategical position of middle powers focussing on cyber. As middlepowermanship is a label that denotes a certain label of cooperation and a multi-stakeholder model, it would flow logically that for any middle power state with an exceptional cyber infrastructure it would be wise to focus on this terrain. Nevertheless, great power politics on one side and regional tensions on the other have the tendency to overshadow said aspirations. The nexus between multilateralism and cyber herein is difficult to strive for. Legislation has not yet been codified and attribution and deterrence are terrains of problems that do not arise when a state focusses on traditional niches such as human rights or trade relations.

By conducting research focussing on the Netherlands and South Korea, it flows logically that cyber is a domain that is woven into the fabric of all aspects of modern society. It is therefore difficult to differentiate between its functional aspects for modern society on the one hand and the military component relating to national security on the other hand. As has been seen in the cases described, geopolitical indicators have the ability to shape cyber power in a way that is out of the hands of the middle power in question. Seoul, is essentially dependent on

[182] Gareth Evans, 'Australia's Foreign Relations in the World of the 1990s'.
[183] Cooper, Higgott, and Nossal, *Relocating Middle Powers*.

international and mainly US policy vis-à-vis North-Korea, drastically decreasing agility. This is telling for middle power theory in the cyber realm in South Korea as opposed to traditional niches, cyber is dependent on a common denominator that in this existential case is fundamentally different for the state versus the broader international community.

On a final note, it is complex to link middle power theory directly to the cyber realm. The middle powers discussed have shown an abundance of initiatives, prestige and motivation to establish themselves in a new policy area. However, as it is with the cyber domain, it has a dominant security component, hereby linking it directly to fundamental security interests of all states, thus also great powers. Great power politics is something that middle powers strive to evade and work around. This makes if complicated for middle powers in the cyber realm to follow a strict multilateral policy aimed at an open and secure cyberspace when openness is propagated on the one hand, while conducting offensive operations notwithstanding the fact that these actions might be for defensive purposes.

Recommendations for further research

In light of this topic of cyber agility, it would be interesting to see further research on the question how middle power theory interacts with policy areas that are of fundamental interest such as the military sphere or water security. The outcomes could then be used to further substantiate the applicability of middle power theory in the cyber realm, which seems to operate in both spheres of regular policy and fundamental security politics.

Future research into this topic should start with further expanding the systemic impact framework. In a next project, tailoring this framework so the complexities and limitations of the cyber realm would allow for more specified analyses. In this way, systemic impact analysis could eventually serve as a useful tool for policy makers.

Next to the elaboration of this framework, applying middle power theory remains complex, due to the absence of a common definition. How fragmented the concept may at this point, the establishment of a common definition by the academic community would greatly increase the value of its conclusions.

Bibliography

Primary sources

David Betz, and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Taylor & Francis Ltd, 2011.

Global Cybersecurity Index 2018. Geneva: International Telecommunication Union, 2019.

Global Forum on Cyber Expertise. 'Framework Document: Launch of the Global Forum on Cyber Expertise 16 April 2015'. The Hague, 16 April 2015.

Korea Internet and Security Agency, 'Korea Internet White Paper 2017'., December 2017.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. 'Jaarverslag AIVD 2018 - Jaarverslag - AIVD'. Jaarverslag, 2 April 2019.

Ministerie van Buitenlandse Zaken. 'Digitaal Bruggen Slaan: Internationale Cyberstrategie Naar Een Geïntegreerd Internationaal Cyberbeleid'. Den Haag, 12 February 2017.

———. 'Mensenrechtenrapportage 2017: Actualisering Buitenlands Mensenrechtenbeleid En Resultaten'. Den Haag, May 2018.

Ministerie van Defensie. '2018 Defence White Paper: Investing in Our People, Capabilities and Visibility', n.d.

———. 'Defensie Cyber Strategie 2018: Investeren in Digitale Slagkracht Voor Nederland', November 2018.

Ministerie van Justitie en Veiligheid. 'Cybersecurity Beeld Nederland 1 December 2011'. Den Haag: GOVCERT.nl, December 2011.

———. 'Nederlandse Cybersecurity Agenda: Nederland Digitaal Veilig'. Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2018.

Ministry of National Defense: Republic of Korea. '2016 Defense White Paper'

Sico van der Meer. Cyber power in The Netherlands and South Korea, 24 October 2018. The Clingendael Institute for International Relations.

Secondary sources

Asser Institute: Center for International and European Law. 'The Tallinn Manual 2.0 and The Hague Process: From Cyber Warfare to Peacetime Regime', 18 February 2016.

Andrew F. Cooper. 'Middle Powers: Squeezed Out of Adaptive'. *Public Diplomacy Magazine*, 2009.

'ASEAN - Republic of Korea Free Trade Area'. ASEAN | ONE VISION ONE IDENTITY ONE COMMUNITY. Accessed 16 April 2019. https://asean.org/?static_post=asean-republic-of-korea-free-trade-area-2.

Baldwin, David A. *Power and International Relations, A Conceptual Approach*. Princeton: Princeton University Press, 2016.

Behringer, Ronald M. 'Middle Power Leadership on the Human Security Agenda'. *Cooperation and Conflict* 40, no. 3 (September 2005): 305–42.

Behringer, Ronald M. 'The Dynamics of Middlepowermanship'. *Seton Hall Journal of Diplomacy and International Relations* 9 (2013): 15.

Campbell, Joel R. 'Building an IT Economy: South Korean Science and Technology Policy', n.d., 9.

Carr, Andrew. 'Is Australia a Middle Power? A Systemic Impact Approach'. *Australian Journal of International Affairs* 68, no. 1 (January 2014): 70–84.

Chanlett-Avery, Emma, Liana W Rosen, John W Rollins, and Catherine A Theohary. 'North Korean Cyber Capabilities: In Brief', n.d., 13.

Cooper, Andrew Fenton, Richard A. Higgott, and Kim Richard Nossal. *Relocating Middle Powers: Australia and Canada in a Changing World Order*. UBC Press, 1993.

Countil of the European Union. 'Non-Paper: Developing a Joint EU Diplomatic Response against Coercive Cyber Operations'. Brussels, 19 May 2016. http://statewatch.org/news/2016/jul/eu-council-diplomatic-response-cyber-ops-5797-6-16.pdf.

Cox, Robert W. 'Middlepowermanship, Japan, and Future World Order'. *International Journal* 44, no. 4 (1989): 823–62.

Cyber Security Raad. Samenstelling, webpage, 9 April 2019, https://www.cybersecurityraad.nl/.

David Betz, and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Taylor & Francis Ltd, 2011.

European Commission. ‘Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace’. Brussels, 7 February 2013.

———. ‘The Directive on Security of Network and Information Systems (NIS Directive)’. Text. Digital Single Market, 5 July 2016. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

‘European Union (EU): Directive No. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data’, 1995. http://www.wipo.int/wipolex/en/text.jsp?file_id=313007.

Eytan Gilboa. ‘The Public Diplomacy of Middle Powers: Navigating the Middle’. *Public Diplomacy Magazine*, 2009.

Finnemore, Martha, and Kathryn Sikkink. ‘Taking Stock: The Constructivist Research Program in International Relations and Comparative Politics’. *Annual Review of Political Science* 4, no. 1 (2001): 391–416.

Gareth Evans. ‘Australia’s Foreign Relations in the World of the 1990s’. Canberra, 4 November 1991.

NETmundial: Global Stakeholder Meeting on the Future of Internet Governance. ‘NETmundial: The Beginning of a Process. Accessed 25 May 2019. http://netmundial.br/about/.

Noort, Wouter van. ‘Hack kost Maersk honderden miljoenen’. NRC Handelsblad. Accessed 11 May 2019. https://www.nrc.nl/nieuws/2017/08/16/petyanotpetya-hack-kost-maersk-honderden-miljoenen-12548891-a1570079.

Hau Boon Lai. ‘Smaller Countries Can Be A Middle Power in East Asia. The Straits Times, 29 August 2013. https://www.straitstimes.com/asia/smaller-countries-can-be-middle-power-in-east-asia-says-top-south-korean-diplomat.

Herzog, Stephen. ‘Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses’. *Journal of Strategic Security* 4, no. 2 (June 2011): 49–60.

Ingo Rohlfing. *Case Studies and Causal Inference: An Integrative Framework*. Palgrave Macmillan, 2012.

Ivan, Paul. ‘Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox’. *European Policy Center*, n.d., 16.

James Andrew Lewis. ‘Advanced Experiences in Cybersecurity Policies and Practices’. Inter-American Development Bank, July 2016.

Jason Healey. ‘Beyond Attribution: Seeking National Responsibility for Cyber Attacks’. Washington D.C.: The Atlantic Council, January 2012.

Jordaan, Eduard. ‘The Concept of a Middle Power in International Relations: Distinguishing between Emerging and Traditional Middle Powers’. *Politikon* 30, no. 1 (May 2003): 165–81.

Ju Yong-Wan. ‘Survey on the Internet Usage 2017’. Ministry of Science and ICT, n.d.

Keohane, Robert O. ‘Lilliputians’ Dilemmas: Small States in Internatinal Politics’. *International Organization* 23, no. 2 (ed 1969): 291–310.

Kim, Euikon. ‘Korea’s Middle-Power Diplomacy in the 21st Century’. *Pacific Focus* 30, no. 1 (1 April 2015): 1–9.

Kim, Si Hong. ‘NAPCI and Trilateral Cooperation: Prospects for South Korea-EU Relations’. Text. IAI Istituto Affari Internazionali, 1 March 2017. https://www.iai.it/en/pubblicazioni/napci-and-trilateral-cooperation-prospects-south-korea-eu-relations.

Klimburg, Alexander. ‘The Whole of Nation of Cyberpower International Engagement on Cyber Establishing International Norms and Improved Cybersecurity’. *Georgetown Journal of International Affairs* 11 (2011): 171–79.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Potomac Books, 2011.

Lee, Kyung Suk. ‘New Approach of South Korea’s Middle Power Diplomacy: Focusing on Global Agenda Setting’. *Global Politics Review* 2, no. 2 (October 2016): 40–57.

Mansourov, Dr Alexandre. ‘North Korea’s Cyber Warfare and Challenges for the U.S.-ROK Alliance’. *North Korea*, n.d., 17.

———. ‘North Korea’s Cyber Warfare and Challenges for the U.S.-ROK Alliance’. *North Korea*, n.d., 17.

McGuffin, Chris, and Paul Mitchell. ‘On Domains: Cyber and the Practice of Warfare’. *International Journal* 69, no. 3 (2014): 394–412.

Melissen, Jan, and Emillie V. de Keulenaar. ‘Critical Digital Diplomacy as a Global Challenge: The South Korean Experience’. *Global Policy* 8, no. 3 (September 2017): 294–302.

Melissen, Jan, and Yul Sohn. ‘Leveraging Middle Power Public Diplomacy in East Asian International Relations’, 2015, 8.

———. ‘Leveraging Middle Power Public Diplomacy in East Asian International Relations’. *The East Asia Institute*, 24 November 2015.

Myriam Dunn Cavelty. ‘Europe’s Cyber-Power’. *European Politics and Society* 19, no. 3 (2018): 304–20.

NCSC. ‘Cybersecuritybeeld Nederland 2017: Digitale weerbaarheid Nederland blijft achter op groeiende dreiging | NCSC’. Webpagina, 14 May 2013. https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2017.html.

‘Netherlands - Embassies and Consulates’. Accessed 15 March 2019. https://www.embassypages.com/netherlands.

Nye, Jr, Joseph S. *Cyber Power*. Cambridge: Belfer Center for Science and International Affairs, 2010.

Oosterveld, Willem, and Bianca Torossian. ‘A Balancing Act: The Role of Middle Powers in Contemporary Diplomacy’. Strategic Monitor 2018-2019. Clingendael Institute, n.d. https://www.clingendael.org/pub/2018/strategic-monitor-2018-2019/a-balancing-act/.

Ravenhill, John. ‘Cycles of Middle Power Activism: Constraint and Choice in Australian and Canadian Foreign Policies’. *Australian Journal of International Affairs* 52, no. 3 (1998): 309–327.

Rijksoverheid. ‘Toespraak Minister Blok over 1-Jarig Bestaan Tallinn Manual 2.0’. Den Haag, 20 June 2018.

Robertson, Jeffrey. ‘Middle-Power Definitions: Confusion Reigns Supreme’. *Australian Journal of International Affairs* 71, no. 4 (4 July 2017): 355–70.

Sangbae Kim. ‘Policy Recommendation for Cyber Security South Korea’s Middle Power Diplomacy:’ Seoul: The East Asia Institute, March 2015.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. 2nd ed. Cambridge: Cambridge University Press, 2017.

Shim, David, and Patrick Flamm. ‘Rising South Korea: A Minor Player or a Regional Power?’ *Pacific Focus* 28, no. 3 (1 December 2013): 384–410.

Sico van der Meer. ‘Cybersecurity Thematic Study Clingendael Strategic Monitor 2017’. The Hague: Netherlands Institute of International Relations ‘Clingendael’, February 2017.

———. ‘Medium-Sized States in International Cyber Security Policies’. *Clingendael Institute*, December 2016.

Singer, Peter, and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2013.

Sliwinski, Krzysztof Feliks. ‘Moving beyond the European Union’s Weakness as a Cyber-Security Agent’. *Contemporary Security Policy* 35, no. 3 (2 September 2014): 468–86.

Tabansky, Lior. ‘Basic Concepts in Cyber Warfare’. *Military and Strategic Affairs* 3, no. 1 (May 2011): 18.

Tae-jun Kang. ‘South Korea Beefs Up Cyber Security With an Eye on North Korea’. *The Diplomat* (blog), 1 April 2015. https://thediplomat.com/2015/04/south-korea-beefs-up-cyber-security-with-an-eye-on-north-korea/.

The Clingendael Institute. ‘A Balancing Act: Strategic Monitor 2018-2019’. Accessed 14 March 2019. https://www.clingendael.org/pub/2018/strategic-monitor-2018-2019/a-balancing-act/.

The Council on Foreign Relations. ‘South Korea’s Difficult Path as a Middle Power in International Cyber Politics’. Council on Foreign Relations, 4 June 2015. https://www.cfr.org/blog/south-koreas-difficult-path-middle-power-international-cyber-politics.

‘The Republic of Korea - Embassies and Consulates’. Accessed 15 March 2019. https://www.embassypages.com/korearepublic.

Wijk, Rob de. ‘Een Kompas Voor Een Wereld in Beweging: De Rol van Buitenlandse Zaken in Het Borgen van Nederlandse Belangen’. The Hague Centre for Strategic Studies, 2017.