Success of Military Alliances Versus Stand-Alone States in Deterring Cyber Threats: The Case of USA and South Korea

By
Alina Shekurova

Submitted to
Central European University
Department of International Relations

In partial fulfillment of the requirements for the degree of
Masters of Arts in International Relations

Supervisor: Christopher LaRoche

Vienna, Austria

2024

Abstract

This thesis explores the application of deterrence in cyberspace and whether this can be done more successfully when the state in question is a member of a military alliance, based on the case of the alliance of the United States (US) and South Korea (Republic of Korea - ROK) and their deterrence against North Korea. This is done through drawing on the traditional scholarship on deterrence theory and its applicability to the cyber domain, as proposed by scholars such as Joseph S. Nye and the scholarship on alliances, such as the works by Edwin H. Fedder and Brett Ashley Leeds. This thesis aims to analyze how four deterrence strategies (punishment, denial, entanglement, and norms) are functioning in the context of the US-ROK alliance, in form of a case-study approach. The US-ROK alliance has a strategic significance for regional security and the member states have an advanced level of technological development. The findings indicate that the US-ROK alliance significantly improves cyber deterrence against North Korea, and is hence more successful than ROK on its own. This thesis aims to present these findings as well as reflect on recommendations for increasing the cyberspace deterrence success in the alliance.

Table of Contents

1. Introduction

In response to the growing threat of cyber aggression, states have sought to develop effective strategies to deter malicious actors from engaging in harmful cyber activities. The core of these strategies is the concept of deterrence, a fundamental principle of international relations theory aimed at dissuading adversaries from taking hostile actions – in this case, conducting cyber attacks -- by demonstrating the capability and willingness to retaliate. Originating during the Cold War era as a response to the security challenges of nuclear weapons, it has seeped into other realms of warfare. Cyberspace has not been an exception. But given the intangible and rapidly evolving nature of cyber threats, the application of traditional deterrence theory to this realm presents unique complexities and uncertainties, which are often seen as an obstacle for its application. As will be demonstrated in the later chapters, some scholars argue against the possibility of applying deterrence in cyberspace as such.

The role of military alliances can be important in cyber deterrence. Military alliances, characterized by mutual defense commitments and cooperative security arrangements, have historically played a central role in shaping states' deterrence postures. By pooling resources, sharing intelligence, and coordinating responses, allied states aim to enhance their collective ability to deter potential adversaries in cyberspace. The effectiveness of military alliances in deterring cyber threats depends on factors like interoperability, information-sharing mechanisms, and the credibility of alliance commitments. In the context of the US-ROK relationship, the military alliance that will be explored in this thesis, is manifested in the Mutual Defense Treaty from the year 1953. Furthermore, the interconnected nature of

cyberspace means that the actions of one state can have far-reaching consequences, underscoring the importance of international cooperation in addressing cyber threats. Additionally, the rapid pace of technological innovation often outpaces regulatory frameworks and policy responses, further complicating efforts to mitigate cyber risks.

Conversely, stand-alone states—those without formal alliance ties—must navigate the complexities of cyber deterrence independently and do not benefit from the power aggregation effects of an alliance. These states rely on their own technological capabilities, diplomatic relations, and strategic communication efforts to deter cyber threats and safeguard their national interests in the digital domain. While stand-alone states may lack the collective defense mechanisms of military alliances, they retain the flexibility to tailor their deterrence strategies to suit their specific cybersecurity needs and priorities. However, this autonomy also brings challenges, as stand-alone states may face resource constraints and limited access to intelligence-sharing networks, which can hinder their ability to effectively detect and respond to cyber threats. Additionally, stand-alone states must contend with the dilemma of maintaining a delicate balance between deterring potential adversaries and avoiding escalation in cyberspace conflicts, where attribution and accountability are often elusive.

Given the situation described above, this thesis aims to explore the dynamics of cyber deterrence within the context of military alliances versus stand-alone states, with a focus on the case of the United States and ROK. The central research question guiding this paper is, therefore: “Do military alliances play a role in application of deterrence in cyberspace, exemplified by the relationship of the US and ROK?” and the initial assumption is that the alliances should be more effective in this regard than stand-alone states. The expectation is that an ally can help its adversary to apply deterrence effectively and increase its success due

to joint capabilities, shared resources, experiences, and military power. This should also apply to cyber deterrence, but perhaps to a lesser extend due to the complicated nature of cyberspace.

By examining the cyber deterrence strategies employed by the US-ROK alliance as part of the Mutual Defense Treaty and the strategies that South Korea implements outside of this treaty as a stand-alone state, this research aims to uncover the nuanced interplay of factors shaping cyber deterrence outcomes. Through a comparative analysis of these two distinct approaches to cyber deterrence, this thesis seeks to contribute to a deeper understanding of how states navigate the challenges of deterring cyber threats in an interconnected world. The case of the US and South Korea has been chosen for this study for different reasons. Both states have a long history of cooperation, the inception of which can be seen in the Mutual Defense Treaty from 1953. The partnership with ROK is one of the most strategically important partnerships of the US in the Asia-Pacific region, which is tightly integrated into the network of partnerships that the US has established there. The alliance of the US and ROK is also a unique blend of civilian and military cooperation. This applies first of all, to the cyberspace, where the states conduct joint cybersecurity initiatives and collaborative research partnerships, such as the Public-Private Cybersecurity Partnership, US-ROK ICT Policy Forum and the Cybersecurity Technology Exchange. Both states are known for a high degree of interconnectedness and advanced technologies, which suggests a high level of possible cyberthreats that can be exemplary and significant for states with less developed technologies that have not reached such level of advancement yet. Advanced technological infrastructure is often a reason why a state can become a prime target for cyber threats, and in case of ROK, one is also bound do consider its complicated geopolitical setting, in which North Korea, a powerful potential aggressor, is located closely and does not shy away from

diverse provocations. These also reach into the cyberspace: it is believed that North Korea has been employing various tactics of impacting ROK's cyber realm, ranging from the DDoS attacks in 2009, attack on hydro and nuclear operations in 2014 and more recent multiple infiltrations into cryptocurrency exchanges. These examples demonstrate the range, as well as the significance of impact: it is known by now that not even the critical infrastructure is safe from cyber attacks. Therefore, ROK has a broad and diverse landscape of cyber threats, which is unique, but may also serve as a manual for other states that suffer from cyber attacks of similar nature. In context of alliance studies and alliance management in other states, the functioning of the US and ROK alliance can serve as inspiration in many aspects, including the cyberspace-related policies, since it has survived various political challenges coming from both participating states and has been evolving since. The experiences of the US and ROK partnership can help policymakers, military strategists, and cybersecurity researchers with various insights into ways of managing cybersecurity as part of alliances and through the states on their own.

The significance of this research lies in its potential to inform policy discussions and decision-making processes related to cybersecurity and international security cooperation, as well as to fill the gaps in scholarship between the concept of deterrence in cyberspace and its practical implications through military alliances. By elucidating the strengths and limitations of military alliances versus stand-alone states in deterring cyber threats, this study aims to offer valuable insights for policymakers, defense planners, and cybersecurity practitioners seeking to improve their states' cyber resilience and strategic posture in the face of evolving cyber challenges.

In the following sections, this thesis will provide a comprehensive review of the existing literature on the impact of military alliances, (cyber) deterrence, establish a theoretical framework for analyzing cyber deterrence strategies, explain the methodology employed in this study, present the findings of the comparative analysis, and discuss the implications of the research for theory and practice in cybersecurity policy and international relations in general. The analysis aims to demonstrate the role of military alliances in deterring cyber threats – specifically, cyber attacks -- and access their contribution to fostering a secure cyber space on the level of states. First, the existing literature will be accessed, followed by theoretical framework, methodology and the analysis of the case.

2. Literature Review

The literature review encompasses the scholarship on the military alliances, their cybersecurity side, the effectiveness of alliances in comparison to lack thereof, as well as the scholarship on classical deterrence and deterrence in cyberspace. The results found shall help in establishing the reasoning and the starting point for the present research.

To establish a thought-out framework for the following analysis, one should consider the understanding of the concept of alliance in literature, as well as its potential influence on deterrence. This, in turn, should help in leading the analysis into the narrower direction of deterrence in cyberspace.

2.1 Alliance

In "An Empirical Typology of International Military Alliances" Bruce M. Russet defines alliance as a "formal agreement among a limited number of countries concerning the conditions under which they will or will not employ military force." (Russet, 1971, 262-289) This narrow definition encompasses the military domain only, focusing heavily on force. Even though this definition may as well be applied to the US-ROK alliance, since it prevents them from employing military force against each other, their alliance is more far-reaching, just as most of the bilateral alliances of the US in the Asia-Pacific region. Joint deterrence-related policies may be interpreted into the idea of non-employment of military force, but as will be demonstrated, its application to the cyber realm requires interference beyond the typical scope of military operations. Another work that discusses alliances on the level of concepts and definitions is "The Concept of Alliance" by Edwin H. Fedder. There, he

discusses various conceptualizations that characterize alliances. He opts for a rather general definition of an alliance as a “limited set of states acting in concert at X time regarding the mutual enhancement of the military security of the members.” (Fedder, 1968, 65-86) The emphasis is placed on military security within alliances, distinguishing them from other forms of international cooperation and highlighting their unique function in safeguarding member states' interests. Furthermore, it allows a distinction between not only military alliances and other forms of international cooperation, but more importantly, between military alliances and other kinds of collective security arrangements, which are manifested through broader means of maintaining security of the members. The most important feature that differentiates alliances from stand-alone states is presence of an agreement on common action or lack thereof. This feature of an alliance is in the core of both mentioned definitions and is vital for understanding of an alliance in context of the present research. To analyze the functioning of deterrence in cyberspace in military alliances and outside of it, the policies implemented by South Korea on its own will be compared to its joint policies and operations with the United States as based on their agreement.

Brett Ashley Leeds defines alliances as "written agreements, signed by official representatives of at least two independent states, that include promises to aid a partner in the event of military conflict, to remain neutral in the event of conflict, to refrain from military conflict with one another, or to consult/cooperate in the event of international crises that create a potential for military conflict" (Leeds, 2003, 427-439). She further delineates five basic promises inherent in alliance agreements: defensive cooperation, offensive cooperation, neutrality, nonaggression, and consultation, noting that alliances often include multiple promises simultaneously. The theoretical underpinnings of Leeds's argument draw from models developed by Morrow, Smith, and Fearon, asserting that formal military alliance

agreements provide crucial information to state leaders about the likelihood of intervention by other states in potential conflicts. This notion suggests a potential link between a concluded military alliance and deterrence.

Fedder conducts a literature review of his own, in which he discusses the plurality of perspectives on alliances present in the scholarship. He references, among others, Morgenthau and Potter, whose contributions permit the expansion of understanding of alliances for the purpose of the present thesis as well. Morgenthau conceptualizes alliance as a mechanism for manipulating equilibrium, emphasizing the assurance of mutual assistance in times of adversity as a central tenet, while Potter views alliance as the "simplest form of international union approaching the forms of international government," underscoring the necessity of formal provisions for collective action, such as a written treaty. Combining the contributions by Fedder, Morgenthau, Ahsley and Potter, one obtains a working concept of an alliance, under which the Mutual Defense Treaty between the US and South Korea can be subsumed - it is an agreement between two states that defines the direction and scope of their cooperation in military matters, and under certain conditions – even beyond. The details of the Mutual Defense Treaty will be explored in the later chapters.

The other, more philosophical insights can further help in establishing a link between an alliance and deterrence. Herbert Dinerstein's scholarship delves deeper into the dichotomy between traditional and contemporary alliances, highlighting the evolution of ideological considerations in diplomatic alignments. (Dinerstein, 1965, 589-601) While traditional alliances were primarily driven by military goals and minimal ideological considerations, modern alliances are characterized by ideological dynamics that significantly shape diplomatic relations. For example, the primary objective of contemporary alliances, such as

the non-Communist coalition led by the United States is containing Communism. Hence, ideological reasoning or foundation can be found in an alliance that in writing only appears to touch the military realm. According to Dinerstein, ideological motivations shape inter-alliance relations among larger and smaller powers (Dinerstein, 1965, 589-601), adding further complexity to alliance dynamics, where the hegemon usually the driving force of the determination of the ideology of their alliance with the smaller power. Deutsch and Kaplan emphasize the strategic calculus in alliance formation. They posit alliances as mechanisms for transforming the international system, particularly during periods of transition from bipolarity to alternative world orders (Deutsch and Kaplan, 1964, 170-171) – this can, perhaps, be best applied to the alliance formation after the WWII, from where the Mutual Defense Treaty originates.

2.2 Deterrence and Cyberspace

This part aims at defining the ties between deterrence and cyberspace as well as juxtapose it to nuclear. Classical deterrence goes hand in hand with nuclear weapons and security issues they have posed since their creation. Nuclear weapons have become a pressing issue in the international politics since their use in 1945. 4 years later, when the USSR developed its own nuclear arsenal, the world appeared soon in the situation of nuclear deterrence between two superpowers. This was the birth of deterrence theory, and what is now understood as classical deterrence. Nuclear deterrence was based on a credible threat of retaliatory attack if an adversary used its own nuclear weapons, which justified the necessity to sustain a certain nuclear arsenal, as well as maintaining and signaling the readiness to put them into use. Classical deterrence is usually thought of in four waves of development, three of which refer to the post WW2 period. The first wave focused on strategic implications of nuclear weapons,

the second incorporated game theory elements into the study of deterrence, and the third wave dealt with the difficulties of the second, such as heavy reliance on deduction. The fourth wave, as suggested by Lupovici, expands the focus to multidimensionality, different actors, development of norms and new technologies, (Lupovici, 2010, 705-732) making it the most accommodating of deterrence in cyberspace. The credibility of threat is one of the reasons why deterrence is considered to be the most successful strategy for preventing nuclear warfare, and which will prove problematic in the cyber domain. However, the theoretical foundation of deterrence can be applied to any other states, and to an arsenal that may be vastly different from the nuclear.

Since the emergence of the cyberspace as a new domain for conflicts, going beyond the scope of simply a new weapon, there exists a debate if deterrence can be applied to it. General line in the scholarship is that deterrence cannot be applied well to cyberspace. Classic deterrence, as mentioned, can be defined as a strategy, the key to which lies in proving to an adversary that the cost of intended harm outweighs the benefits, and consists of "a threat or action designed to increase an adversary's perceived costs of engaging in particular behavior, and an implicit or explicit offer of an alternative state of affairs if the adversary refrains from that behavior." (Trager and Zagorcheva, 2005, 89-90.) The article by Joseph S. Nye Jr., Deterrence and Dissuasion in Cyberspace, suggests broadening the classical concept of deterrence by mechanisms of norms and entanglement, and proposes that deterrence in cyberspace can work if certain aspects will be improved (Nye, 2016-17, 55). Since each of the four means of deterrence (punishment, denial, entanglement, norms) are parts of the deterrence concept, it is important to explore them regarding their applicability in cyberspace.

Nye considers punishment – should the threat of retaliation come to life -- as one of the two primarily mechanisms of deterrence. However, he assumes that punishment is considerably less effective in cyberspace. (Nye, 2016-17, 55) Nye blames it, primarily, on the nature of cyber attacks that resembles crime rather than nuclear aggression. (Nye, 2016-17, 45) Most cyber attacks are low-scale in comparison to armed conflicts, and are often mere provocations, as it is the case with cyberwarfare of North Korea against South Korea (Platte, 2020, 75-94), which will be discussed further. This already makes the cyber attacks hard to deter. But complications are also provided by unclear effects and consequences of cyber attacks. It is demonstrated by the case of STUXNET, in which a virus was used to destroy Iranian nuclear centrifuges back in 2012. The scholarship cannot agree if it fully equated to an act of classical warfare (McGraw, 2013, 109-119) or was an example of pre-emptive deterrence by punishment (Iasiello, 2018, 37). Cyber operations are complicated and hardly traceable, which makes attribution of an attack rarely possible.

Furthermore, uncertainty about the effect of cyber weapons contributes to the lack of proper signaling of threat and capabilities, which hinders the fear of punishment: it is not clear if a certain actor is able to carry out the threat. According to T. Schelling, for deterrence to function, effective communication (which includes signaling) is required between the actor that deters and the one that is being deterred (Solomon, 2011, 2). This notion ties together intransparency of capabilities and lacking attribution in cyberspace, which make deterrence by punishment ineffective. Nye's suggests that deterrence can work with certain attribution. He talks about the threat of retaliation that deterred Hitler from using chemical weapons against Britain or the United States and no-first-use declarations (Nye, 2016-17), suggesting that similar scenario may enhance cyber deterrence. But chemical and nuclear weapons are vastly different in destructive and fear-inducing effects from cyberweapons and are far more

transparent. Nye's suggestion does not demonstrate the practical possibility to improve deterrence by punishment in cyberspace.

Regarding denial, Nye suggests it is "indifferent to attribution" (Nye, 2016-17, 53), which makes it more effective than deterrence by punishment. There is no agreement on the perspective of deterrence by denial in cyberspace in literature: while Platte suggests that denial cannot prevent all attacks (Platte, 2020, 86), especially the low-scale ones, Iasiello argues that denial has high chances to succeed in cyber space (Iasiello, 2018, 49), albeit with improved defense capabilities. Nye, too, recognizes that success of deterrence by denial depends on the quality of defense capabilities, but follows a different trope in his analysis: according to him, it's not denial, but already improved defense capabilities that would reduce the incentive for cyberattacks. Innovatively, he notes the link of defense to intransparency of the offense, which complicates the improvement of the former (Nye, 2016-17, 56-68). Intransparency and uncertainty are therefore limiting to both punishment and denial. In conclusion, the scholarship is more hopeful about denial since it doesn't require attribution and can be enhanced by improving defense capabilities. But since there is still imbalance between offense and defense, the full potential of denial is hindered.

This leads to Nye concentrating on "broader" deterrence means: that by norms and by entanglement, even though the rest of the scholarships is rather skeptical about them. Although it is suggested that the need to broaden the original concept of deterrence by weaker forms to apply in cyberspace speaks for its inapplicability (Fischerkeller and Harknett, 2017, 387), Nye offers arguments as to why it is worth doing so. Norms work in favor of outweighing the benefits, since they can impose high costs when they are broken, which is indeed true in case of the nuclear weapons. This yet again refers to problematic

attribution in cyberspace: who is bound to bear the price of abusing a norm, cannot be seen without possible attribution. No attribution of attacks means no adherence to the norms that forbid them. Nye admits that establishing norms is hard but proposes that if it's not possible to forbid cyberweapons due to their interchangeability and fast development, it is at least possible to forbid certain types of targets (Nye, 2016-17, 61) and hence, make the laws of cyberwarfare more like those of armed conflicts, which would contribute to their effectiveness. But deterrence by norms is still not applicable to states such as North Korea that cannot be deterred by possible reputational damages that come from abusing norms. Fischerkeller and Harknett, moreover, deem it unachievable to establish norms for cyberspace due to operational restraint policy (Fischerkeller and Harknett, 2017, 393), as it is the case with the U.S. Hence, despite Nye's optimism, deterrence through norms may not work well due to a set of different reasons.

Nye suggests that entanglement contributes greatly to deterrence in cyberspace. The key of entanglement is interdependence that has come into place in our modern globalized age. Due to this, the harm that an actor is willing to cause to another one, will impose costs on him as well, and the costs may equate or outweigh the harm that he is willing to cause. This finds support in the case of the U.S as the carrier of the largest number of nodes in the structure of global interdependence. Also, Richard A. Clark and Robert K. Knake, note that "the U.S. probably should be deterred from initiating large-scale cyber warfare for fear of the asymmetrical effects that retaliation could have on American networks." (Clarke and Knake, 2010, 189) This refers to the concept of self-deterrence, which is used by Nye in accordance with its definition by R. Jervis (Nye, 2016-17, 59). Nye argues that the perceptions that can be wrong can also be accurate, and this argument points towards the uncertain and ambiguous nature of cyberspace and signifies that entanglement can work only in certain, non-definable

circumstances. Furthermore, the literature does not explore how entanglement may deter actors that are not interdependent with others to a large degree (for example, North Korea) (Platte, 2020, 19). Thus, entanglement is also not a fully functioning mean of deterrence in cyberspace.

While most authors elaborate on two classical means of deterrence, Nye offers close elaboration on the other means of dissuasion. He proposes that despite certain difficulties, all means of deterrence can be applied in one way or another when it comes to cyberspace. This does not find large support in other literature and is partially contradicted by his own arguments. Nevertheless, one may admit that even if the concept of deterrence (neither broad nor classical) can be fully adopted to cyberspace, some elements and instruments might as well be useful in certain scenarios in cyber domain. Therefore, when analyzing the way deterrence in cyberspace is exercised through military alliances, one should keep in mind that the widely accepted four means of deterrence (punishment, denial, entanglement, and norms) generally have a limited functionality in this case.

Speaking of deterrence in alliances, Brett Benson's research is worth mentioning. Benson's work underscores the significance of alliances in shaping deterrence strategies, particularly in distinguishing between alliances formed to compel adversaries to take specific actions and those established to deter them from certain behaviors, such as defense alliances. Benson classifies alliances based on their objectives and occurrences that shall trigger military intervention. Based on this, alliances can be categorized into unconditional and conditional compellent alliances, as well as unconditional and conditional deterrent alliances. He also introduces a fifth category, probabilistic deterrent alliances, which allow members to potentially escape obligations once hostilities have commenced. In a deterrent alliance, in

particular, there is no active interaction with a hostile adversary, but rather setting a stage and waiting for his action, whereas compellent alliances initiate actions based on the opponents' response. In a deterrent alliance, B and C seek to preserve the status quo by threatening A with negative consequences if it attacks. In forming an alliance, B and C set the stage by establishing a threat to defend the status quo. They then wait, and the tripwire is triggered if A takes action to change the status quo. Successful deterrence implies A's inaction when such an alliance is present (Benson, 2011, 1111-1127). Based on this example, the assumption is that A is less likely to initiate a militarized dispute against B if B is a party to a conditionally deterrent alliance. In terms of applicability to the Mutual Defense Treaty, which will be investigated later, one may stick to the conditional deterrent type. Benson argues that successful deterrence occurs when adversaries refrain from taking hostile actions due to the threat of negative consequences posed by alliances. He suggests that conditional deterrent alliances, especially those involving minor powers and major power defenders, are particularly effective in deterring violent militarized conflicts. Furthermore, only conditional deterrent alliances, which explicitly promise allied intervention in the event of an attack, are successful in deterring violent conflicts, which is most favorable for the smaller power.

In conclusion, one can see the tendency in the scholarship to omit the connection "Alliance – deterrence – cyberspace," whereas the connections "alliance -- deterrence" and "deterrence -- cyberspace" exist and are well explored. Using the insights from the scholarship, this thesis aims to tie the strings together and expand on it through exploring the effectiveness of cyber deterrence in military alliances, using the example of the US and South Korean Mutual Defense Treaty.

3. Theoretical Framework

To answer the question whether alliances play a role in success of cyber deterrence in cyberspace, this chapter will place the Mutual Defense Treaty and the relationship between the US and South Korea in line with the concept of deterrence, including the four deterrence means: punishment, denial, entanglement and norms.

3.1 Deterrence Conceptualization

Classical deterrence theory relies heavily on the threat of retaliation, which would often return in the same realm, as in case with the nuclear weapons. The threat must also be credible: if it cannot be believed and taken seriously, it will not be able to dissuade the actors from hostile actions. These are the main issues in application of deterrence to cyberspace. As observed by Josepf S. Nye, cyber attacks are seen as manifesting through low-scale incursions that cannot be surely attributed to a certain adversary. Therefore, punishment is hardly a well-functioning strategy for deterrence in cyberspace.

The challenges of punishment might be solved through application of alternative approaches, the next one suggested being the denial. Preventing or mitigating impact of cyber attacks through improving defense capabilities to an extend that the attacks will become predictably unsuccessful may be more effective than the strategy of punishment. However, this implies the possibility to ensure quality of defense mechanisms and test them in practice. This would endanger the secrecy of the mechanisms, which is usually required in the entire military sphere and is decisive for success of any strategy. Furthermore, the ambiguity of the cyber

realm does not allow an establishment of an equilibrium between the offensive and defensive capabilities, as explored by Platte and Iasiello.

Logically, the lacking application of the two strategies above inspire to think of other strategies, such as norms and entanglement. As discussed by the scholars above, such as Nye, as well as Fischerkeller and Harknett, norms may help deterrence through imposing costs on violators. Norms may include laws and regulations, which either define a material fine, or cause heavy reputational damages in case of their violation. They also serve as a guidance and code of conduct, based on which the proper type of behavior in cyberspace can be defined. However, the significance of a fine or reputational damage may not be serious in the perspective of a certain adversary, which would diminish the effect of the norms almost to the fullest. But even before the issue of the impact of a norm arises, the issue of attribution can make it impossible to determine who the norm is to apply to in the first place.

Entanglement is also a flawed strategy when it comes to cyberspace. It implies interdependence inside of a certain set of actors, that are interconnected in a way that not only concerns technologies, but also their economical coexistence. In theory, the consequences of threats and actual attacks in cyber domain may reach far into other domains, threatening an actor in a way that the provoker or the attacker suffers from them as well. Hence, both the perpetrator and the target have to carry the cost, which may deter the perpetrator from the provocation or the attack. However, entanglement demonstrates flaws, as noted by Platte, when it comes to the not-so-entangled actors. North and South Korea serve as a good example of states with no interdependence despite their geographical and historical proximity, largely due to the isolationist policy of the North and ideological discrepancies. An actor like North Korea is knowingly independent and does not openly rely on international

cooperation, especially with the US or South Korea, and hence cannot be threatened by its own actions against these actors.

3.2 Mutual Defense Treaty

Mutual Defense Treaty from the 1st of October 1953 is the founding treaty of the US – South Korea alliance. According to the preliminary statement the purpose of the treaty, and hence of the alliance, is among the rest to "strengthen the efforts for collective defense for the preservation of peace and security pending the development of a more comprehensive and effective system of regional security in the Pacific area." The parties settle to solve disputes peacefully (Article 1), consult in case of a threat of an armed attack (Article 2) and act together on common dangers (Article 3). When it comes to security and joint means to ensure it, there are not plenty provisions or detailed regulations on the matter. Article 4 merely stipulates that South Korea grant the US the right to dispose its "land, air and sea forces in and about the territory of the Republic of Korea as determined by mutual agreement." This implies the necessity to conduct separate agreements on more specific matters and policies, which then can be seen complementary to the present, broad agreement. Interestingly, the treaty contains a disclaimer – a provision named "Understanding of the United States," which asserts that according to the US, the parties of the treaty should only be obligated to come to aid to each other solely in case of an external armed attack, which has been "recognized by the United States as lawfully brought under the administrative control of the Republic of Korea". The same applies to any assistance provided by the US to South Korea.

Returning to the concept of alliance, one may see that the agreement, on paper and de facto, is a vital element of an alliance and any kind of joint actions. In this case, the treaty has left space for integrating various elements and policies into the alliance activities through mutual agreement. However, the scope of the alliance is strictly defined and is restricted exclusively to military realm and defense actions, whereas in practice it arguably was, and remains a nuclear alliance, heavily focused on nuclear deterrence. In this context, deterrence can be seen as part of the joint defense policy. It does not explicitly fall under the scope of the treaty, since it is not triggered by a specific external armed attack. However, it is encompassed by the purpose of the treaty and the alliance to "strengthen the efforts for collective defense." Collective defense means that deterrence provided by South Korea in favor of its own state and extended deterrence provided by the US ("dissuasion of adversary actions against a third party or non-immediate interests," (Brantly, 2018, 34) are equally important for security of the two allied states.

In cases when the treaties are concluded for an unlimited period of time, as it is the case here, they are composed in a purposefully vague formulation to ensure their viability and adaptiveness to the new realities. It is clear that in 1953 the parties would not necessarily think of including deterrence into the treaty. It is a concept that only started developing its modern shape during the Cold War era and was not in focus at the time of conclusion of the Mutual Defense Treaty, where it rather seemed more important to codify the common side of US and South Korea in the competition of two polar world orders. The treaty and the alliance themselves are means of deterrence, which can also explain the vague and "threatening" wording, as well as the obligation to help in case of an armed attack without defining the kinds of attacks and the conditions under which the obligation will apply. To conclude, deterrence in cyberspace falls into the scope of the founding treaty and the alliance, even

though it is not explicitly regulated by it, since the treaty serves as the framework and manifestation of intent for the future, narrower agreements.

4. Methodology

This research is based on the case study approach. The study of application of deterrence in cyberspace through alliances and stand-alone states, as well as the comparison of both is only possible when a certain pair of states is taken as an example. An in-depth exploration of a case in context of said theoretical foundations helps deepen the understanding of their practical implications and access their contribution to real life. A case can also offer valuable insights and lessons for similar situations and help cybersecurity professionals in various fields handle the same problems and their respective states. The insights for this study can be drawn through qualitative content analysis of academic literature, policies, documents, expert opinions and interviews, where the nature of the matter must be taken into account.

Deterrence as a strategy requires certain expression to the outside world and thought-out sharing of specific information: for example, one is required to openly talk about increased defense capabilities or let them be known otherwise to dissuade another actor from the attack (denial). If the potential attacker is not aware of (presumably) sufficient defense capabilities of another actor, he cannot access its own offensive potential and decide it the attack will be successful. However, in case of cyber capabilities, revealing defense capabilities may reveal information about offensive capabilities as well, or jeopardize cyber policy otherwise – for example, through allowing the enemy to learn from the information received. Therefore, when analyzing the revealed information on deterrence-related projects in cyber space and opinions on their success, one should consider the situation and purpose why a certain claim is made. For this reason, various sources will be used, and different perspectives will be incorporated. An in-depth interpretation and the comparative analysis that follows will help reach the conclusion if cyber deterrence works more successfully as a joint action of the US and South Korea or if South Korea could be just as successful on its own.

As mentioned, the reasons for choosing South Korea and its alliance with the US are multi-faceted. South Korea as a stand-alone state has a high level of interconnectedness and technological development, which increases the level of cyber threats that it has to face. Answering the question what kind of actions are deterred against and who is the main target of the deterrent actions, the focus will be put on North Korea and its cyber activities with a malicious intent and considerable impact on South Korea. North Korea is located in a dangerous geographical proximity and has been frequently called out by South Korea for its actions, as in the Ministry of National Defense's (MND) 2016 Defense White Paper (Republic of Korea Ministry of National Defense, 2017, 77-79). Furthermore, cybercrime is an essential tool to ensure financial survival of Kim's dictatorship, allowing it to fund its weapons programs, and hence plays a greater role than for some other cybercrime-conducting states (Antoniuk, 2023). For these reasons, this research is heavily focused on deterring North Korean threats, despite the presence of other potential targets such as China. Aside from nuclear threats, which remain the traditional aim of deterrence in the case of South Korea as well, it has to deter the provocations of North Korea in the cyber domain. In this context, the presence of the US in the region in form of an ally does not only offer practical support to South Korea, but also contributes to the regional stability and balance of power. In cyber realm, both states have a great degree of cooperation, which provides an example for other states that may aim to increase their own international relations.

5. Analysis

5.1 Realities of South Korea's Cyberspace and South Korea's Deterrence

() South Korea has a turbulent cyber space landscape. The number of daily cyber attacks targeting government offices alone ranges from 1 million to 1.4 million (Baek, 2023), and the state is number five in the worldwide statistics of significant cyber attacks from 2006 to 2020. (specops, 2020) The most significant cyber attacks on South Korea (attributed to North Korea) include repeated data breaches, a hacking attack on the Nuclear Research Agency in 2021, and the data theft from the Defense Ministry in 2018 (Top 15 Cybersecurity Breaches in South Korea). Although the damage could be contained and did not disrupt any essential services, as it was the case with earlier cyber attacks as well, there was agenda and motivation behind the attack. In the cyber domain, South Korean scholars write that North Korea's primary aim is "to attack the intelligence network when there is a total war to delay the intervention of U.S. Troops." (Lee et al., 2019, 438) It is also argued that North Korea could "first conduct a simultaneous and multifarious cyber offensive on…society and basic infrastructure, government agencies, and major military command centers while at the same time suppressing the ROK government and its domestic allies and supporters with nuclear weapons." (Platte, 2020, 75-94) Cyber capabilities of the attacker and the degree of control he is able to exercise is always devastating, and it seems to be a question of time when North Korea's cyber capabilities will reach a more serious level, aside from the dangerous potential of combining attacks in multiple domains at once. Although definite attribution of the attacks to North Korea is not possible, ROK often does it based on the timing of the attacks. In a nutshell, the frequent cyber provocations have caused South Korea's preparation for a full-fledged cyber war with the North (McGraw, 2013, 109-119).

South Korea has various projects aimed at increasing its cybersecurity on its own, as well as part of the cooperation with the US. Part of its strategy is apparently the open disclosure of the pursued means. The three strategic drivers of the South Korea's policy as of 2024 according to the Institute for National Security Strategy are the determination of threat factors, reaffirming its responsibilities as a Global Pivotal State to promote safe cybersecurity space, and clearly outlining the domestic cybersecurity governance (Kim, 2024). The state's awareness of the need to raise its cybersecurity potential is also seen in the readiness to invest in the information security sector: the aimed spending in this sector by 2027 is 1.1 trillion won ($827.1 million), which is double the budget over the past four years. The South Korean approach involves various ventures, such as attraction of think tanks, formation of a domestic security belt, as well as expansion of a training center for cyberattacks and defense in Pangyo. The state aims to effectively include new technologies such as AI, adopting the Zero Trust strategy in the network security that means constant verification of all connected terminals to ensure that no attacks are happening on them (Kim, 2023).

Aside from recognizing threats such as state-sponsored hacking organizations, technology leakage and incapacitation of critical infrastructure, large focus is given to North Korea, to which the theft of classified information, dissemination of false information, and cryptocurrency theft is attributed (Kim, 2024). The new strategy also highlights collaboration with the US, especially the Strategic Cybersecurity Cooperation Framework, which will be discussed further in context of the US-South Korea alliance. Already in 2019, South Korea's National Cybersecurity Strategy has defined a set of means directed at improving the resistance towards cyber vulnerabilities. The first task is to strengthen security of national information and communication networks, which includes implementation of basic security

measures, regular inspections, expanding back-up facilities, ensuring compliance with worldwide technical standards as well as advancing cryptographic systems. Regarding the critical infrastructure, the strategy aims to improve schemes of its protection, such as authentication infrastructure, increasing the budget for its security and compose standards for security evaluation based on the unique nature of each infrastructure type. Furthermore, the strategy also focuses on cyber attack response capabilities, and here the document explicitly uses the word "deterrence:" in this sense, the strategy is to "actively respond to all cyber attacks that infringe upon national security and national interests by concentrating national capabilities," "Strengthen preventive capacity by building a system that efficiently collects, manages, and eliminates vulnerabilities in cyberspace," as well as "acquire practical capabilities to analyze causes of cyber attacks and identify the culprits." (Kim, 2024) The strategy also recognizes the importance of increasing readiness against massive cyber attacks, using AI-based technologies and public-private-military cooperation and joint drills. Other means of increasing cyber readiness involve plans for quantitative classification of cyber crises to increase response capabilities through the private sector and continue focusing on cybercrimes. The state also aims to develop countermeasures for cyber attacks, on which it is not elaborated further. It is stated, however, that in order to achieve that, South Korea is planning to reinforce military strength, acquire core technologies and train cyber warfare specialists. This strategy echoes the ICT Strategy Committee of the Ministry of Science and ICT, which in 2021 proposed a Cybersecurity Promotion Strategy. It suggested, among others, following means: ensure real-time detection and sharing of cyber threats, provide 1,300 companies with 300 contactless solutions and 110,000 cases of cybersecurity assessment, Build robust cybersecurity systems for the four key digital convergence technologies (5G MEC, cloud, data, and post-quantum cryptography) ahead of demand and invest KRW 670 billion by 2023 to raise Korea's cybersecurity level to the world's top 5

(”The 13th Meeting of the ICT Strategy Committee Was Held,” Press Release of the Ministry of Science and ICT).

South Korea has established various organizations and runs different initiatives that contribute to the fulfillment of the states’ plans regarding its cybersecurity. One of such organizations is the Korea Internet & Security Agency (KISA) that among other functions runs the national incident response team and delivers international trainings in cybersecurity. The Global Cybersecurity Center for Development (GCCD) works on increasing cybersecurity worldwide through collaborating with international organizations such as the World Bank, with which it has funded the provision of national capacity assessments (Collett and Barmpaliou, 2021, 17). Another effort is the Smart Ship Cybersecurity Demonstration Project from 2023, which helped increase the scope of analysis of cyberthreats in maritime industry by 400% (Safety4Sea, 2023). Furthermore, the Korea Internet & Security Agency (KISA) has launched a common cybersecurity project “ASEAN Cyber Shield” with the ASEAN member states for common enhancement of cyber capabilities (Seon, 2023).

Overall, South Korea’s National Cybersecurity Strategy and the Cybersecurity Promotion Strategy combine means to increase technological defense capabilities, improve nation-wide as well as international cooperation, strengthen critical infrastructure, information-sharing system, as well as normative basis to regulate the current and emerging threats. There is a common course throughout different institutions, which is significant of good coordination and engagement with the topic of cybersecurity.

Regarding South Korea’s strategy against specifically North Korean cyber threats, a more proactive approach is expected to be adopted over the upcoming years. There is an awareness

that not all threats can be minimized, and that cryptocurrency is one of the most complicated paradigms for cybercrime prevention. So Jeong Kim, the director of emerging security studies of the Institute for National Security Strategy, frequently emphasizes the importance of international cooperation to develop successful responses to North Korean cyber threats, stressing importance of joint projects with the US (Kim, 2023). To start their exploration, one should start with the most important document that the two states have produced in the recent years.

5.2 Extended Deterrence as Part of the US-ROK Alliance

Deterrence posture of the US-ROK alliance nowadays is encompassed by the concept of extended deterrence - deterrence, provided by the US on behalf of ROK, which is becoming increasingly proactive and focuses on strategic attacks of a higher scale, whereas the lower-scale attacks should be deterred by South Korea on its own. strategic attacks could include North Korean use of nuclear, biological, or chemical weapons or a large-scale, conventional attack on South Korea (Platte, 2020, 75-94). The joint communique from the 2017 U.S.-ROK Security Consultative Mechanism (SCM), an annual meeting between the US Secretary of Defense and the ROK Minister of National Defense, proclaimed that the United States would provide extended deterrence “using the full range of military capabilities, including the US nuclear umbrella, conventional strike, and missile defense capabilities.” (Joint Communiqué of the 49th ROK-U.S. Security Consultative Meeting, U.S. Department of Defense, 2017) These general features of the deterrence posture mostly apply to cyberspace deterrence as well.

The Strategic Cybersecurity Cooperation Framework between the US and South Korea from April 2023 defines the new course for the alliance with regard to cybersecurity. The states intend to make cybersecurity a high policy priority and reaffirm their desire to continue their cooperation established in 1953, although not being a legal document itself. The document explicitly stresses the need to expand the strategic alliance into the cyberspace, the lack of which has often been a point of criticism in the past. According to the Framework, the states "intend to begin discussions regarding how the Mutual Defense Treaty would apply and under what circumstances." (Strategic Cybersecurity Cooperation Framework Between The Republic Of Korea And The United States Of America, 2023) It also explicitly mentions deterrence by stating the indent to cooperate on "deterring malicious cyber activity" with tactics from the Joint Statement from May 2022. These included deepening cooperation with regard to critical and emerging technologies, defending human rights online, developing secure 5G and 6G networks and supply chain security (United States-Republic of Korea Leaders' Joint Statement, 2022). Overall, the Framework is consisted of basic principles, such as defending common values, promoting a stable cyberspace, securing cryptocurrency operations and supporting military cyber operations. It also lists the mechanisms for joint cybersecurity activities, such as the U.S.-ROK Cyber Dialogue and the U.S.-ROK Working Group on DPRK Cyber Threats, as well as best practices and research exchange through various institutions like the U.S. Cybersecurity and Infrastructure Security Agency's Joint Cyber Defense Collaborative (JCDC) and the aforementioned KISA. Although both states do not widely and publicly discuss military cyber operations, they have been carried out in the past years, and are carried out nowadays. The combined military exercise Ulchi-Freedom Shield (earlier Ulchi-Freedom Guardian) has been carried out since 2015, and 2023 was not an exception – designed to strengthen the combined defense posture ("The Republic of Korea and United States announce exercise Ulchi Freedom Shield 23, America's Navy", 2023), it

promotes interoperability in all domains including cyberspace. It has been an important part of the exercise in the past as well: for example, in 2016, the total of 80 000 soldiers trained in keeping a secure cyber network for their own communication, resolving incidents and strategic issues (Durr, 2016). Operation Freedom Shield in March 2024 also aimed at joint defense posture improvement and focused on cyber domain to the same extend as on the other domains (”Freedom Shield 24 set to begin,” 2024). Other operations include Key Resolve, directed at crisis management in context of operational planning warfighting (“Exercise KEY RESOLVE”, 7th Air Force,), Foal Eagle, focused on rear area security and stability operations (“Exercise FOAL EAGLE”, 7th Air Force), as well as Cyber Storm – a U.S. initiative, where international partners including ROK take part. The exercises include simulation of cyber incidents, coordination and incident responses (”Cyber Storm: Securing Cyber Space,” America’s Cyber Defence Agency).

In 2020 the Joint Communique of the 52nd U.S.-ROK Security Consultative Meeting has reached the expansion of cyber defense, artificial intelligence, automation, and directed energy (Joint Communique of the 52nd U.S.-Republic of Korea Security Consultative Meeting, United States Forces Korea, 2020). Strengthening the ROK-U.S. alliance is mentioned in the 2023 Progress Report of the ROK’s Indo-Pacific Strategy. According to it, the countries have significantly strengthened extended deterrence provided by the U.S. This statement requires further study: what does one make of the means and strategies described above in context of cyber deterrence and how useful is the U.S.-ROK alliance in this regard?

5.3 ROK/US Alliance: Challenges for Extended Deterrence and Cyberspace

There are various challenges that the US-ROK alliance faces when applying deterrence in cyberspace. These challenges are not typical for nuclear deterrence, but arise in context of cyberspace, and arguably cannot be diminished even through applying deterrence in framework of an alliance with a trusted and powerful strategic partner. The US army researchers, based on their practical experience, admit that attack attribution is a problem even in the well-established military domain when it is merged with cyber domain (Caton, 2019). For example, the first-strike advantage that cannot be deterred, furthermore, there is a risk of asymmetric vulnerability to attack in cyberspace. The risk tolerance in cyberspace can also be different and less predictable than it is with actions in the physical domain (Caton, 2019). Additionally, Dr. Dorothy Denning challenges several other fundamental aspects regarding cyber deterrence. Cyberspace, like any other domain, is a combination of natural and manufactured structures. Hence, deterrence focuses on influencing decisions and actions and the human elements of this process. She also asserts that "the principles that have made nuclear deterrence effective for over half a century fall apart in cyberspace." (Dennings, 2015) She emphasizes the important difference between cyberweapons as a deterrent tool and other, non-offensive means that fall into cyberspace. However, new technologies can increase the success of extended deterrence in cyberspace, where both the efforts of ROK as a stand-alone state (e.g., through investment) and joint efforts of the alliance (e.g. through joint research) play a big role. As former Deputy Secretary General of NATO Rose Gottemoeller expressed in 2014, "Extended deterrence [by US to ROK] . . . contains within it a full panoply of weapons systems and everything that goes with weapons systems to make them effective." (Edmonston, 2022, 9) Thus, technologies may be able to improve intelligence so that both ROK and the US-ROK alliance can better anticipate and attribute the cyber threats of North Korea, in a shorter period of time than it is currently possible.

Another issue of cyber deterrence, threat credibility, remains a problem independently of whether the threat is expressed by a stand-alone state or by an alliance. While nuclear deterrence has a credible threat in its core, it primarily addresses high-level provocations and does not effectively deter North Korea's lower-level provocations, which frequently occur in cyberspace. To address these cyber threats, the alliance has established a relatively new Cyber Cooperation Working Group aimed at tackling the full range of cyber issues. If this working group becomes integrated into the Extended Deterrence Policy Committee (EDPC), it could expand the approach to cyber deterrence. It remains to be seen how effective the working group will be, but it has potential to increase the cyber competence of the alliance and increase credibility (Manning, 2014, 13-15). In this regard, one can see progress in comparison to the past. For example, the 2011 White House document, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, outlines an ambition to "work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation." (McKenzie, 2017)

Furthermore, declaratory policy in both nuclear and cyber realms can play a significant role in deterrence. Given the history of cyber intrusions from North Korea, a US-ROK joint statement reserving the right to respond to hostile cyber actions—especially those damaging critical infrastructure or causing loss of life—with kinetic countermeasures, could enhance deterrence. This kind of policy formulation could also be considered for the destruction of space assets, adding another layer to the deterrence strategy.

The issue can be solved through threatening retaliation in other, more "fearful" and credible domains. This is where US can prove to be a useful ally with its experience, human resources and a highly developed military domain. For example, as suggested by Michael Edmonston, "knowledge of what we can "see" via RPA-borne ISR would frighten North Korea by the threat of what the US-ROK alliance can do in response" (Edmonston, 2022, 2-14). This response can come in various forms without having to restrict itself to cyber domain. But if an attack is carried out in cyber domain, it can still have an advantage in comparison to the nuclear realm: an attack in cyberspace can be carried out multiple times without having as much of a destructive impact as a nuclear attack. Therefore, one can assume that the issue of credibility may be diminished by repetition and combination of different acts (Edmonston, 2022, 2-14), which can also be intensified by the strategy of extended deterrence.

An unsolvable challenge seems to lie in application of entanglement and norms. North Korea has a reputation of being nearly immune to sanctions and does not adhere to international law. For actors that play by the rules, advocate for human rights and promote democracy like the US and ROK do, it may be hard to play against an actor who doesn't, since they cannot use the same kind of means. North Korea also diminishes the opportunity to respond with a cyber attack to a cyber attack, since North Korea is not interconnected with the rest of the world, practically isolated, and is not very target-rich environment with not enough military hardware, bases, or major infrastructure that could be vulnerable to a cyber attack. North Korea has even been called the cyber equivalent of Afghanistan (McGraw, 2013, 109-119). In this case, it is not detectable how an alliance such as the US-ROK can be more successful in these means than a stand-alone state such as South Korea.

One can observe that the US can indeed contribute to security of South Korea through extended cyber deterrence against North Korea using its influence, reputation, technological advancements and military capabilities. The role of the US can thus be well summarized as follows: deterrence in cyberspace can be achieved "through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems." (Caton, 2019, 34) The next chapter explores this in context of each mean of deterrence: punishment, denial, entanglement and norms.

6. Discussion

The discussion aims at exploring how the 4 strategies of cyberspace deterrence are applied in ROK and US-ROK alliance in more detail. This will lead to conclusion if the US-ROK alliance is valuable in increasing their success.

The strategy of cyber deterrence by punishment within the USA-ROK alliance faces a lot of criticism. However, there are plenty options that have potential, if the alliance figures out how to manage the flaws of this strategy to increase its success rate. The strategy of punishment includes such means as information operations, disruption of military networks, economic sanctions as well as infrastructure strikes. These means could carry a strong message and be well executed using the power and resources of the US. The negative aspect of lacking timely and convincing attribution can be diminished in the future with advancing technologies and with the present awareness of this issue among the alliance member states. Ensuring that retaliatory measures are appropriate and proportional to the severity of the attack is crucial to avoid unnecessary escalation and international condemnation. But the issue of balancing the target of retaliatory action and the original trigger will always stay in the discretion of the applying state and its ambiguity belongs to the nature of international politics. Thus, it is worth concentrating on attribution as well as on credibility of threat and sending the right and loud message about willingness to carry out the attack. Joint initiatives and official statements in a certain tone, as well as research on increasing attributive capabilities can contribute to solving this issue. The previous parts have demonstrated that the US-ROK alliance is following precisely this course of action.

The strategy of cyber deterrence by denial within the USA-ROK alliance focuses on enhancing the resilience and robustness of critical networks and systems to prevent adversaries from achieving their objectives, increasing redundance of critical networks and improving supply chain security. Denial is a strategy that is heavily focused on defense, which implies increasing defense capabilities through developing the state's own technologies. The aim is to increase defense capabilities to a level that will raise the failure rate of an attack to make it obsolete. This strategy implies always staying ahead of technological capabilities of the potentially dangerous actor, but the lack of information on the capabilities of that actor (especially if it follows an isolationist policy like North Korea) makes it hard to know of the reached degree is enough to provide a powerful enough defense. It is argued that it is ineffective and "has permitted North Korea to enjoy operational freedom to choose the time and place of its attacks without fear of retaliation." (The Asian Institute for Policy Studies and Center For Strategic & International Studies, 2013) But despite this, it can still be applied to cyber domain – and can almost be applied automatically through increasing defense capabilities. This can be seen in development efforts and research projects of ROK, as well as in international cooperation that helps increase cybersecurity of many like-minded actors.

Deterrence by entanglement may come through increasing dependence on interconnected networks. This can also help with tracking malicious activities and hence improve attribution. Using deterrence by entanglement could open new, perhaps undiscovered ways of deterring cyber threats. However, with actors like North Korea, where the degree of entanglement with other actors is either low or non-trackable, there are little reasons to hope that entanglement can contribute to the overall deterrence posture. This is demonstrated by the lack of means

implemented by ROK as well as the US-ROK alliance that focus on North Korea's interconnectedness.

Deterrence by norms could work through applying laws of behavior in cyberspace or proposing cyberspace conflict-managing mechanisms. Norms may deter states that are not as provocative as North Korea and that adhere to international norms. Which is why, despite ROK's general strategy to contribute to promotional of international norms and standards for cyberspace, it is directed at creating a positive reputation worldwide and contributing to the worldwide cyberspace security.

In total, the combination of traditional means (punishment and denial), as well broader means of entanglement and norms, can be applied to cyberspace when the applying state manages to improve attribution, credibility of threats, as well as impose influence on the adversary to make it adhere to norms and entangle itself with the worldwide interconnected networks. Placing the right focus and priority on the attacks to deter can help decide which strategy to apply. Thus, the mixture of means applied can differ for ROK and the US-ROK alliance based on their strengths and weaknesses, as well as strategic importance and scale of threats. As well summarized by James E. Platte, an overall strategy for the US-ROK alliance should contain of fostering their cooperation and forming an organized joint cybersecurity command. As has been explored in the previous chapters, the alliance is working in this direction. Military capabilities and their clever integration into the cyber domain, as well as the weight of US definitely contributes to the success of deterrence application, which makes it more powerful that ROK's posture on its own. This can be well exemplified by the cyber-military realm, where it is nearly impossible think away the role of the US. US as an ally can therefore be seen as a deterrent element of its own, that primarily increases the role of deterrence by

punishment (signaled through official documents threat of retaliation, starting with the Mutual Defense Treaty) and denial (increasing ROK's defense capabilities through joint trainings and providing resources). The same can be said about the states reaffirming openly their continuing cooperation, which is just as important as was its initial announcement in 1953.

The success of deterrence application in cyberspace through the alliance depends on the capabilities of the member states, which means one should not ignore the capabilities of ROK as a stand-alone state. Understanding the value of US as strategic partner as well as being well aware of the constantly evolving North Korean threat in the cyber domain, ROK has adopted a multifaceted approach that focuses on international cooperation and investing in technological development. However, in face of the threats posed by North Korea, the capabilities of ROK on its own are admittedly not enough. It can be concluded that an alliance with powerful enough capabilities can be beneficial for cyber deterrence, but there are certain recommendations on how to improve. The alliance could switch to a more proactive deterrence and rely less on denial while focusing on North Korean strategy. It is considered that the doctrine of proactive deterrence would "preclude actual war-engagement, dissuade North Korea from planning provocations, and press North Korea to rely on non-violent means to achieve its ends." (The Asian Institute for Policy Studies and Center For Strategic & International Studies, 2013) The member states could also concentrate on the domestic political landscape of South and North Korea in determining alliance strategy. Moreover, the member states should reaffirm its devotion to cooperation in multiple domains and inform the public more openly and strategically effective about their joint cyber deterrence posture – for example, through releasing a comprehensive U.S.-ROK cyber deterrence statement or document. In deterrence itself, the alliance should focus on deterring

North Korean cyber attacks that have strategic effects or could enable strategic attacks, not particular types of cyber weapons or attacks, and center the actions below the level of an armed conflict (Platte, 2020, 75-94).

7. Conclusion

This thesis has aimed to explore if an alliance can help diminish some of the classical problems that arise when applying deterrence in cyberspace. The specific focus on the role of US-ROK alliance in increasing the effectiveness of deterrence application in cyberspace and its four means (punishment, denial, entanglement and norms) has served to demonstrate the complicated nature of the issue. With the lack of precise information on technicalities of cyber defense and offense of the respective states, a statistic connecting deterrent actions and frequency of North Korea's cyber provocations, as well as with a lacking mathematical framework to measure success of deterrence, one could only rely on opinions, observations and speculations. However, even in this situation it was possible to derive certain differences in deterrence application of ROK and the US-ROK alliance. These include the amount and scale of operations, technological capacities used and experience combined. The weight and expertise of the US are essential for addressing sophisticated cyber threats. Joint initiatives, such as the U.S.-ROK Cyber Dialogue and the U.S.-ROK Working Group on DPRK Cyber Threats, contribute to information sharing and help coordinate responses to the threats. Deterrence means implemented through the US-ROK alliance seem to be the most effective in context of punishment and denial, since these strategies can be improved by the efforts of the member states to a larger extend than it is the case with entanglement and norms. Formal alliance ties serve as a stable basis for future collaborations and agreements that define the scope of future commitments and contribute to the deterrence effects already at the stage of their conclusion. Therefore, it can be concluded that a well-developed and managed alliance can increase the success of deterrence application in cyberspace.

Bibliography

Antoniuk, Daryna, ”FBI: North Korean hacking group Lazarus behind $100 million crypto heist,” The Record, 25.01.2023 https://therecord.media/fbi-north-korean-hacking-group-lazarus-behind-100-million-crypto-heist

Baek, David Sehyeon, ”Overseas Market Expansion for South Korean Cybersecurity Companies: Challenges and Opportunities,” 01.12.2023 https://www.linkedin.com/pulse/overseas-market-expansion-south-korean-cybersecurity-companies-baek--vuvhc/

Benson, Brett, ”Unpacking Alliances: Deterrent and Compellent Alliances and Their Relationship with Conflict, 1816–2000,” The Journal of Politics , Vol. 73, No. 4 (Sep. 14, 2011), pp. 1111-1127

Brantly, Aaron F., “The Cyber Deterrence Problem,” Proceedings of the 10th International Conference on Cyber Conflict, NATO Cooperative Cyber Defence Centre of Excellence, 2018, 34

Bruce M. Russet, “An Empirical Typology of International Military Alliances,” Midwest Journal of Political Science, May, 1971, Vol. 15, No. 2 (May, 1971), pp. 262-289
Caton, Jeffrey L.,”The Army Role in Achieving Deterrence In Cyberspace,” Strategic Studies Institute, US Army War College (2019)

Clarke, Richard A., and Knake, Robert K., “Cyber War: The Next Threat to National Security and What to Do About It”, New York: HarperCollins, 2010, 189.

Collett, Robert, Barmpaliou Nayia, ”International Cyber Capacity Building: Global Trends and Scenarios”, Annex 3, Notes on Cyber Capacity Building Funders, 2021, 17

-------,”Cyber Storm: Securing Cyber Space,” America’s Cyber Defence Agency https://www.cisa.gov/cyber-storm-securing-cyber-space

Dennings, Dorothy D., ”Rethinking the Cyber Domain and Deterrence,” JFQ 77, 2nd Quarter 2015

Deutsch, Karl W. and Kaplan, Morton A., "The Limits of International Coalitions," in James N. Rosenau, ed., International Aspects of Civil Stife (Princeton: Princeton University Press, 1964), pp. 170-171.

Dinerstein, Herbert, "The Transformation of Alliance Systems," The American Political Science Review, 59 (September, 1965), pp. 589-601

Durr, Robert N., “Ulchi Freedom Guardian -- Defending the Cyber Network”, U.S. Army, 12.09.2016
https://www.army.mil/article/174934/ulchi_freedom_guardian_defending_the_cyber_network

Edmonston, Michael, ”The Impact Of RPA Technology On Conventional Deterrence On North Korea,” The Maxwell Papers, Air War College, 2022, 9

-------, ”Exercise FOAL EAGLE,” 7th Air Force https://www.7af.pacaf.af.mil/About-Us/Fact-Sheets/Display/Article/408383/exercise-foal-eagle/

-------, ”Exercise KEY RESOLVE,” 7th Air Force https://www.7af.pacaf.af.mil/About-Us/Fact-Sheets/Display/Article/408384/exercise-key-resolve/

Fedder, Edwin H., “The Concept of Alliance,” International Studies Quarterly, Mar., 1968, Vol. 12, No. 1 (Mar., 1968), pp. 65-86

Fischerkeller, Michael P. and Harknett, Richard J., “Deterrence Is Not a Credible Strategy for Cyberspace”, Elsevier Ltd for Foreign Policy Research Institute, 2017, 387

”Freedom Shield 24 set to begin”, United States Forces Korea, 27.02.2024 https://www.usfk.mil/Media/Press-Products/Press-Releases/Article/3688893/freedom-shield-24-set-to-begin/

Iasiello, Emilio, “Is Cyber Deterrence an Illusory Course of Action?”, ASPJ Africa & Francophonie – 1st Quarter 2018, 37

Joint Communiqué of the 49th ROK-U.S. Security Consultative Meeting, U.S. Department of Defense, October 28, 2017 https://dod.defense.gov/Portals/1/Documents/pubs/20171028-Joint-Communique-OSD-MND-October-17-Final-version.pdf

Joint Communique of the 52nd U.S.-Republic of Korea Security Consultative Meeting, United States Forces Korea, 14.10.2020 https://www.usfk.mil/Media/Newsroom/News/Article/2382466/joint-communique-of-the-52nd-us-republic-of-korea-security-consultative-meeting/

Kim, Jin Won, ”S.Korean gov't to invest $827 mn in cyber security sector by 2027,” The Korea Economic Daily, 06.09.2023 https://www.kedglobal.com/business-politics/newsView/ked202309060008#:~:text=A%20cybersecurity%20fund%20worth%20%2497.7,develop%20unicorns%20in%20related%20industries&text=South%20Korea%20will%20invest%201.1,over%20the%20past%20four%20years

Kim, So Jeong, ”ROK’s New National Cybersecurity Strategy and Its Implications,” Issue Brief Vol. 106, No. 3, 2024

Kim, So Jeong, ”South Korea’s Capacity Building against North Korean Cyberthreats,” interviewed for the National Bureau of Asian Research, 19.12.2023 https://www.nbr.org/publication/south-koreas-capacity-building-against-north-korean-cyberthreats/

-------, ”Korean project comes up with best practices for cybersecurity regulations,” Safety4Sea, 07.12.2023

https://safety4sea.com/korean-project-comes-up-with-best-practices-for-cybersecurity-regulations/

Leeds, Brett Ashley, "Do Alliances Deter Aggression? The Influence of Military Alliances on the Initiation of Militarized Interstate Disputes," American Journal of Political Science , Jul., 2003, Vol. 47, No. 3 (Jul., 2003), pp. 427-439

Lee et al., "The Countermeasure Strategy Based on Big Data against North Korea Cyber-attacks," 2019, 438

Lupovici, Amir, "The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda," International Studies Quarterly , September 2010, Vol. 54, No. 3 (September 2010), pp. 705-732

Manning, Robert A., "Reassuring Korea: The Future of US Extended Deterrence in Asia to 2025," Atlantic Council (2014), 13-15

McGraw, Gary, "Cyber War Is Inevitable (Unless We Build Security In)", Journal of Strategic Studies, 36:1, 109-119, 2013

McKenzie, Timothy M., "Is Cyber Deterrence Possible? Analysis of Current US Cyber Policy," Air University Press (2017)

Mutual Defense Treaty Between the United States and the Republic of Korea; October 1, 1953
https://www.usfk.mil/Portals/105/Documents/SOFA/H_Mutual%20Defense%20Treaty_1953.pdf

Nye, Joseph S. Jr, "Deterrence and Dissuasion in Cyberspace", International Security, Vol. 41, No. 3 (Winter 2016/17), 55

Platte, James E., "Defending Forward on the Korean Peninsula", The Cyber Defense Review, Vol. 5, No 1,International Conference on Cyber Conflict, November 18-20, 2019: Defending Forward (Spring 2020), 75-94

Republic of Korea Ministry of National Defense, 2016 Defense White Paper, Seoul: Ministry of National Defense, 2017, 77-79

Russet, Bruce M., "An Empirical Typology of International Military Alliances," Midwest Journal of Political Science, May, 1971, Vol. 15, No. 2 (May, 1971), pp. 262-289

Seon, Han Gyeol, "KISA launches ASEAN Cyber Shield project for strengthening cyber security," The Korea Economic Daily, 31.01.2023
https://www.kedglobal.com/tech,-media-telecom/newsView/ked202301310005

Solomon, Jonathan, "Cyberdeterrence between Nation States: Plausible Strategy or Pipe Dream" Strategic Studies, Quarterly 5, No. 1, 2011, 2

-------, STRATEGIC CYBERSECURITY COOPERATION FRAMEWORK BETWEEN THE REPUBLIC OF KOREA AND THE UNITED STATES OF AMERICA, 04.2023

https://www.president.go.kr/download/644956452f9e3#:~:text=OF%20CYBERSECURITY%20COOPERATION-,The%20Republic%20of%20Korea%20and%20the%20United%20States%20of%20America,including%20the%20sharing%20of%20intelligence.

-------, The Asian Institute for Policy Studies and CENTER FOR STRATEGIC & INTERNATIONAL STUDIES, ”Future of ROK-US Alliance,” Asan Institute for Policy Studies (2013)

-------, ”The countries experiencing the most ‘significant’ cyber-attacks," specops, 09.07.2020 https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/

-------, ”The 13th Meeting of the ICT Strategy Committee Was Held,” Press Release of the Ministry of Science and ICT https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=489&searchOpt=ALL&searchTxt=#

-------, “The Republic of Korea and United States announce exercise Ulchi Freedom Shield 23”, America‘s Navy, 14.08.2023 https://www.navy.mil/Press-Office/Press-Releases/display-pressreleases/Article/3491680/the-republic-of-korea-and-united-states-announce-exercise-ulchi-freedom-shield/

-------, ”Top 15 Cybersecurity Breaches in South Korea” https://www.cyberlands.io/topsecuritybreachessouthkorea

Trager, Robert F. and Zagorcheva, Dessislava P., “Deterring Terrorism. It can be done”, International Security 30:3, 2005, 89-90

-------, United States-Republic of Korea Leaders’ Joint Statement, 21.05.2022 https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/21/united-states-republic-of-korea-leaders-joint-statement/