TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Kseniia Neradko

A CYBER WESTPHALIA: CHALLENGING THE FIFTH DIMENSION

Bachelor's Thesis
Programme International Relations

Supervisor: Vlad Vernygora, MA

Tallinn 2018

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 11229 words from the introduction to the end of summary.

Kseniia Neradko ……

(signature, date)

Student code: 156186TASB

Student e-mail address: nera.kseniya@gmail.com

Supervisor: Vlad Vernygora, MA:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

The aim of this research work is to argue that the way different countries and international organizations interact with each other in the field of cyber security makes the political geography-linked Westphalian paradigm obsolete. More significantly, this process is cobbling the road to a new paradigm – perhaps, it could be called 'cyber-Westphalia' – since the Internet and information technologies have already provided for an anonymous, borderless but dangerous type of threat to be real.

This paper is focused on identifying the cyberwarfare concept and its characteristics. It discusses the main foreign and domestic policy implementations conducted by both major powers and smaller states. A closer look at a range of NATO – originated cyber security directions and mechanisms is offered, too. The paper evidently confirms the international system's shift towards a more definite form of collective defense, cyber security wise. In general, this research is an attempt to add some value of the process of observing the actual complexity of the cyber threat that can, with necessity, lead to the enhancement of cooperative combating methods against it.

Keywords: Cyber security, cyber space, cyberwarfare, cyber attack, cooperation

Cyber-warfare, not unlike other means of twenty first century warfare, is coming of age in an era where the Westphalian state order is undergoing vast transformation.

Rex Highes, A treaty of cyber space

The cyber domain is likely to increase the diffusion of power to non-state actors and illustrates the importance of networks as a key dimension of power in the 21st century.

Josepfh Nye, Cyber Power

INTRODUCTION

Our world is featured by constant development and changes. The field of Information Technologies (IT) is probably at the summit of development in the contemporary century. Not only did the Internet as a communicational platform become an integral part of life, but it was also managed to simplify interactions between countries, in business and across cultures, while bringing up a range of revolutionary opportunities for education and healthcare. It could be argued that the emergence of the cyber space as a separate domain represents the most important outcome of the IT-originated development. Certainly, on the disciplinary level, Political Science (in general) and International Relations (in particular) as an academic discipline directly affected by these changes. On the one hand, as argued by Geers (2011, 97), this brings benefits in terms of improving the communication systems and motivating for the creation of the new strategies. On the other hand, there is the new type of threat coming from the cyber space. It is the new arena of conflict where the basic defense and attack strategies are still unclear (Geers 2011, 97).

Cyber security is the subject of concern for the world political society due to the increased accessibility of the internet. Moreover, the IT is constantly expanding in both developing and developed counties.

The Stuxnet attack was the turning point for many scholars in evaluating the real threat of the cyber space. The malicious attack on the Iranian nuclear power plant that targeted computers controlling the centrifuges; it did not stop until they accessed the 'DNA' computer of the nuclear reactor (Demchak and Dombrowski 2011, 32-33). The attackers were able to compromise work of the nuclear program, affected the work of the computers and lead to the centrifuges to destroy themselves. Thus, the attack revealed the strategic danger of the cyber space. The cyber attack on Estonia in 2007 also revealed the danger for the security of one country. It proved that the cyber space can indeed be used for expressing opposition to the decision of the government and achieving the certain political goals. It affected work of the banks, governmental organizations and compromised the ministerial websites. The attack showed to the world society that the great damage for the country can be caused without using the tanks and artillery (Kozlowsi 2014, 238).

On a specific note, the internet opens wide range of possibilities. However, its usage not always legal and brings potential risk for the society. The cyber space features allow the attacker to achieve maximum results. First of all, it offers absolute anonymity for the attacker, so that it absolutely impossible to claim responsibility for committing the attack. Moreover, the geographical borders do not matter. In order to organize the hack, the attackers need only the Internet access, computer and IT skills. On the basis of the numerous cyber attack of a different level of damage scholars began to argue wheatear the cyber space is the new dimension of war. Some scholars support that claim. And confirm the existence of the shift from the conventional warfare to the cyber space. For example, Geers (2011, 97) argues that the ground war will be accompanied with the invisible battle between states using the IT sphere to reach the settled strategic goals. However, other scholars believe that there is no shift towards the cyber space warfare. Thus, Rid (2012, 10) notes that none of the existent cyber attacks meets the requirements for the war due to the absence of violent, political and instrumental threat and consequences. He believes that the cyber attack is more or less is political crime than the act of war (Rid 2012, 10).

Nonetheless, the majority of scholars disagree with the Rid's view on the subject. The cyber attack can indeed cause serious damage to the economy of a country. It can also affect the healthcare and social spheres leading to the real physical damage for the society. Moreover, the attacks are never limited in the actions thus they can attack the nuclear and electric power systems causing the

‘apocalypses’ without energy and heat for days or weeks. Therefore, Nye (2013, 331) believes that the new theater of threat has already emerged in interconnected and interdepend modern world and the governments are most vulnerable targets.

The existence of the so-called 5th Dimension of War does bring threat to the world society. Every country is equally vulnerable within the cyber space. In case of the real threat there are specific procedures and armory ready to protect the state. However, in case of the cyber attack it almost impossible to foresee, prevent and protect the country from it. The borderless and multi-layered Internet became one of the most powerful instruments nowadays that is lacking governmental regulations (European Commission, High Representative of the Union 2013, 3). The unique features of the cyber threat drive the countries and the International organizations such as North Atlantic Treaty Organization (NATO) to collect the knowledge and strategies in order to defeat from the global problem. Thus, many scholars support the idea that the global cyber threat of today is an extra push for the cooperation growth between states. The same way the World War I was the fight of all against all, but also, paradoxically, a global framework for high-level cooperation. Hence, the cyberwarfare is a global threat on the hand, but, on the other hand, it is the new background for cooperation, the balance of power and the world order (Nye 2013, 338).

The new kind of threat requires the innovative preventive methods and defend strategies. Thus, the existing cyberwarfare encourages the cooperation between states and international organizations. This, in turn, will bring the innovative elements to the existing international regimes in terms of the new principles of the conflict recognition and the following reactions. The new battlefield means the necessity of establishing the new territorial borders. The states have to adjust their foreign policy principle and norms. Based on these changes the Westphalian system of the international world order will have to adapt (Demchak and Dombrowski 2013, 30).

Considering the above, this paper claims that **cooperation between different countries and international organizations in the field of cyber security makes Westphalia obsolete.** Methodology wise, this paper is featured by a range of qualitative research methods. The documentary analysis is the source of the data used for discussing the theoretical background of the cyber space and cyber security. Moreover, it helped to enrich the quality of the main argument, present the real

proofs of the growing cooperation on the different levels. The case studies of the USA, China, New Zealand and Australia used to exemplify the argument, make the details more visible. It also helps to identify the most important concepts and bring them to the research. According to (Neuman 2014, 42), the case studies bring not only bring detailed story to the research but also help to have a look on a bigger picture of issue and its background.

The thesis discusses the cyber space as the new dimension of the warfare, its positive effect in the international cooperation and restructuring of the current world order. The paper answers the question of what cyber warfare and its main characteristics. Moreover, the thesis examines the political reactions of the major world hegemonies and NATO on the cyber threat. It also discusses the measures implemented by the smaller countries such as New Zealand and Estonia to defeat their national cyber space. Finally, the paper answers its main question, whether there is growing cooperation in terms of cyber security and if it actually changing the existing world order.

The first chapter of the thesis discusses the theory behind the cyberwarfare, its main characteristics. It also discusses the reactions of the international relations theories on the phenomenon. The second chapter is based on the political implementations, new strategies and the overview of the cyber security by the world powers such as the United States of America and China. The following chapter analyses the reactions of the smaller states such as New Zealand and Australia, their policy implementations and the overall approach towards the new kind of threat. The succeeding chapter presents the findings and proves the existence of the cooperation calls within the International Organizations such as NATO. The next chapter concludes the discussion and presents the final findings. It discusses the cooperation growth in the modern political arena. It also argues for the shifting of the world order from the Westphalian principle to the new one mainly focused on the cyber space. The conclusive chapter summarizes the arguments presented in the thesis. Also discusses the probable research questions and topics for the further scholarly discussion.

1.DEFINING THE CYBERWARFARE

Cyber space is a relatively young and under-researched notion. Its rapid developing and changing character add more challenges for the understanding of the phenomenon. The thesis discusses the war and attack within the cyber space. It is necessary to mention that there are different activities in the cyber space from cyberterrorism to espionage and hacking. The following paper talks only about the cyberwar and attacks connected with it. In order to start analyzing the existing cyberwarfare, its challenges and following changes, it is necessary to clarify the meaning behind these notions. The following chapter discusses the definitions of the cyber space and cyberwarfare and its characteristics. Moreover, the section reflects the reactions and explanations of the notion from the international relations theories point of view.

To begin with, it is important to define the meaning behind the 'cyberwarfare'. What is more important is to analyze the word 'cyber space' separately from 'warfare'. When one says 'cyber' one necessarily thinks about the Internet, artificial intelligence and IT. This, in turn, is fair. However, mentioning the term 'cyber space' brings challenges for the clear understanding of the meaning behind. The notion does not have a universally confirmed definition. Rebecca Bryant (2001, 139) quoting Gibson who early in 1994 defined the cyber space as

> (…) a consensual hallucination experience daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. (…) A graphic representation of data abstracted from the banks of every computer in the human system.

However, the notion revolutionized since that time. However, the thesis adheres to the definition authorized in the UK Cyber Security Strategy, "cyber space is an interactive domain made up of digital networks that is used to store, modify and communicate information, it includes the internet, but also the other information systems that support our businesses, infrastructure and services" (10 Steps to Cyber Security 2012, 3).

It is important to note that the cyber space consist of the Internet, computer network and virtual reality. The domain is borderless. So that any actor can freely "enter" and "move" within the space (Bryant 2001, 139). Moreover, the cyber space allows an open communication not only between individuals via e-mail communication, for example. But, also, the data exchange and storage on the external carries. The cyber space is highly accessible that brings both advantages and disadvantages. On the one hand, it easies many things from learning benefits to finding the new work opportunities for individuals, business and governments. On the other hand, its accessibility and openness threat the personal data and even national security. Thus, a single cyber attack can destroy the business and reputation or cause a serious damage to the nation-state. For example, the Sony Cyber attack and its aftermath. The company's computer network was compromised, personal and corporate data has been stolen. The Sony's reputation was put to the test. The President Obama characterized the attack not only an act against the Sony itself and its employees but also as an attack against the American values and freedom of expression (Theohary 2015). Thus, the attack officially confirmed to be an act against the national security even though the private corporation fell under the attack.

When it comes to the definition of 'cyberwarfare', the complexity of the notion remains. It is a frequently used word today, however only few can define an actual meaning behind it. Some scholars believe that conflict in the cyber space does not qualify to be called 'war'. According to Velriano and Maness (2014, 348), cyber conflict is the usage of the technologies in cyber space for destructive purposes in order to impact, change, or modify diplomatic and military interactions. Clausewitz's theory and understanding of war are the main proves they bring. The classical definition of war is "an act of violence meant to force the enemy to do our will" (Clausewitz 1976,90). The scholar also believes that the physical damage and destruction should necessarily follow the gun power usage. However, it is important to mention that the cyber war is indeed the new type of war. Therefore, due to the nature of the cyber domain there is a different kind of violence. Thus, the human life losses will not necessarily follow the attack (Isnarti 2016, 154). Moreover, the fact that the cyber attacks may one day reach the point when the failure of the attacked systems can indeed because civilian deaths should also be considered. However, it is just an assumption.

The main aspect to be mentioned is the political and military objectives behind the attacks. The cyberwar has nothing to do with economically driven hacking, or the attacks done for fun. Cyberwar is the conflict within the cyber space where the computer network operations apply (Liff 2012, 404). The challenging aspect of the cyber warfare is the absence of physical state borders. The state can exercise its jurisdiction against physical subjects related to cyber space (such as computers and routers) (Couzigou 2018, 41). However, when it comes to the legislations and the war convention procedures the situation is different. Westphalia treaty clearly stated physical borders of the states that still exist today. However, there is no document confirming the state borders within cyber space. According to Bebber (2017, 429) the global norms and jurisdiction are required to increase effectiveness of the actions and bring positive changes to solve the cyber space question. The cyber space is the new domain of the conflict. The conventional methods of warfare, defense and defeat do not apply within the domain. There is an indirect usage of force and the new generation of weapons. However, the intentions behind remain the same as for the conventional conflict.

1.1. Theoretical aspects

Cyber space is a relatively new concept in the international relations. Its rapid development challenges the study and research of that field. The uniqueness and complexity of the phenomenon attracted attention within the political and scientific fields. The notion is still in the stage of researching, thus lacking some clear understanding and scholastic explanation. Due to that fact, there may be not enough explanations International Relations theories wise. However, the following chapter brings the most recent findings on the topic. Moreover, it discusses the IR theories reactions to the cyberwarfare notion.

1.1.1. Neorealism

Neorealism theory in International Relations focuses on the structure of the international political system and its development. Neorealists argue for the anarchy in the internarial political world (Waltz 1990, 29). Also confirming that the state all are equal by nature, however, the capabilities they have differ. Moreover, according to neorealism, states have the greatest authority. Thus, the military attacks can happen anytime, and no one guarantee that one state will not attack another (Isnarti 2016, 155).

Due to that, the states try to maximize their military, economic and political capabilities in order to be ready for any kind of attack. These are the characteristics of so-called defensive neorealism. The cyber space is characterized by the absence of the hegemon or the great power. Moreover, there is an anarchy in the new domain, as there is no higher institution to control the state's actions. Thus, the events and countries' behavior can be explained from the defensive neorealism point of view. Moreover, the weak defensive systems and position of the defender activates the "offensive - defensive balance". Glaser and Kaufmann (1998, 7) argued that the offensive-defensive balance characterized with the situation when "states decisions based on expectations of how structural constraints will mold military outcomes, requires the broad approach because these expectations are often influenced by factors in addition to technology".

Isnarti (2016, 156) offers three main proves why the offensive neorealism can explain the emergence if cyberwar. First on is the cost-effectiveness of the existing offensive cyber weapon ready to protect the state from the cyber attack. As if it would be cheaper and more efficient than creating and constructing the defensive mechanism against the existing threat. Secondly, the failure of the defensive strategies is obvious. The cyber attack targets not only one computer in the country, it is attacking the infrastructure, individual, businesses and the government. Thus, the neorealist belief in equality of states applicable again. The USA or Russia have the great military and defense technologies but still remain the most frequent targets of the cyber attackers. However, the neorealist theory does not explain the probable redistribution of power not only between states but also between other actors (such as private hackers, sponsored cyber organizations and movements).

When it comes to the Westphalia and neo-realism theory, scholars believe that the sovereign model established with the treaty was the starting point for understanding the international environment (Krasner 2001,22). Westphalia plays an important role in the neo-realism theory. The treaty clearly confirmed the necessity and compulsion of having the clearly set borders of the states. Which are interconnected with the fundamental ideas of the neo-realism. Moreover, the treaty plays an important role in the development and sustaining of the theory. When it comes to the cyber space and the absolute absence of the state border, neorealism theory fails to explain its basics. The anonymous and absolutely open nature of the cyber space makes it difficult to apply any of the neo-realism ideas on the issues occurring within the new dimension. Moreover, it is difficult to apply the defensive-

offensive theory. Due to the fact, that as there are no borders to defend and no threat to cause to the other state. According to Tuthill (2012, 20), the classic Westphalian paradigm exists and helps in terms of providing the physical defense for the country. However, when it comes to the cyber security the new understanding and interpretation are needed.

1.1.2. Constructivism

The international relations theory of constructivism is different from other classical theories. First of all, it does not recognize the state as the main actor in international affairs. Moreover, constructivist believe in the structure and construction of the world order. As the states are individual systems with the artificial constructions. Moreover, constructivist explain the word order through knowledge and ideas. Kant, for example, believed that the knowledge one has is filtered through its mind and therefore subjective. The perception of the events necessarily depends on the personal ideas of the individual. The same applies to the state leaders and the country's identity on the world arena. Thus, identity is one of the main concepts for constructivists. They also emphasize norms and cultural aspects as necessary constituents of the international system.

When it comes to the understanding of the cyberwar through the constructivism, it is necessary to understand how the phenomenon is socially constructed. First of all, the development of technologies and internet contributed to the cyberwar emergence. The nature of the threat changed, it shifted from the physical domains of sea and land to the cyber space. On the basis of the previous attacks and their consequences for the nation states, their infrastructure, economic and governmental fields changed the overall perception of fear (Isnarti 2016, 160). Thus, with the changed nature of fear towards the cyber space, the understanding of who is the enemy and how to defend yourself changed too. Moreover, the problem of identity is changing. Thereby, the constructivists believe that there will be no need to conduct cyber war if all actors would gather together to discuss norms and perception. As well as establishing the mutual respect and cooperation.

Westphalia treaty and its main points are necessary for understanding the concepts of constructivism. However, the treaty's concepts play more behavioral model rather than analytic assumption (Krasner 1995, 123). The ideas and understanding of the state and the basics of international relations go hand in hand with the sovereignty concept stated in the treaty. However, in the cyber space where nature of

the state, its borders and expected behavior of the actors are not yet set, constructivism theory struggles to understand the issues. In the absence of the state definition in the cyber space, constructivism cannot fully apply its fundamental ideas and concepts for the better understanding.

1.1.3. Liberalism

The liberalism as one of the classical international relations theory mainly argues for the cooperation, peace and economic stability through it. The theory also confirms the existence of multiple actors in the world political system such as international institutions and organizations. The war is more likely to happen only between the actors who do not cooperate on the economic and social levels. Moreover, the states must be democratic, as their society and government do not have any interest in conflict and losses of a different kind. However, it is necessary to remember that in case of the external threat even liberal societies tend to get involved in the conflict. It happens not only due to the necessity of defending the national borders but also due to the need for the human right protection (Isnarti 2016,158). Only in a totalitarian state where the government is driven by the power and financial hunger the war is likely to happen (Burchill 2005, 60).

When it comes to the cyber space, the liberal ideas tend to prevail. First of all, the democratic states do not attack each other. For example, the Russian cyber attack against the US presidential campaign. Russia is not democratic states that attacked the US that is one the most democratic and free states for today. At the same time, China and Russia do not attack each other. The liberalists point of view here is that the states with the identical or same ideologies never attack each other. Moreover, the recognition of not only state actors but also institutions and organizations by the liberalists highly applicable to the cyberwar. According to what was mentioned before in the introductory part of the thesis, the states not the only attackers in the cyber space. Non-states actors get more power and influence in the highly technological war domain, they also can play the key role in the event of the cyber attack (Sigholm, 2). When it comes to the cooperation and interdependence liberalism theory also applies. However, for now, states and international organizations only discuss the question of the cooperation strategies. The necessity of having one is obvious and inevitable. As according to the liberalists, the interdependence and cooperation on the institutional level tend to decrease the probability of conflict between actors. However, there is still question how the liberalist norms and ideas will work with the cyberwar (Isnarti 2016, 158).

On contrast, liberalism struggles to explain how the liberal states will recognize each other in the new domain. What is more, the basic idea of the theory is the peaceful coexistence between states in the international political environment. Westphalia treaty clearly differentiates the sovereign states and respectively their borders. However, the new cyber dimension lacks the above discussed sovereign borders. Liberalism strongly supports the idea of the sovereignty and its absolute importance. The cyber space does not set any state actors nor accepts the existence of the sovereign at the moment. What is more, liberalism confirms the existence of the non-state actors in the international relations. Westphalia treaty lacks explanations and ideas regarding the role of the international organizations in the political environment. When it comes to the cyber space, there are non-state actors. They not only exist within the new domain. But actively act and cause issues such as cyber attacks and espionage. Thus, liberalism theory together with the Westphalian principles cannot fully explain principles of the cyber space.

1.2. Outcomes

Contextualizing the outcome of this chapter with the paper's argument, the cyberwar and its emergence can be explained from different perspectives. Cyber war is the conflict in digital domain where nation states borders are not yet set. However, cyber space is the subject of the national law of each country (Couzigou 2018, 41). However, there is no existing treaty to set the borders like Westphalian Treaty did. None of the above-mentioned theories can explain all the aspects of the cyberwar. When it comes to the neorealist theory, it explains the ideas and intentions behind conducting the cyberwar. However, it fails to suggest what criteria's the world power should have within the cyber space. Constructivists believe in identities and norms as the main objectives for the establishing principles of the international relations. However, the uniqueness of the phenomenon may become a challenging aspect of identifying these objectives. Liberalists form their perspective can explain the prevention and defending methods for the cyberwar. However, due to the novelty of the cyber space domain, the offered methods may have different consequences as for the conventional conflict.

To sum up, the international theories are connected with the Westphalia treaty. Their fundamental concepts and ideas are interconnected with the concepts of sovereignty and articular state borders. When it comes to the new dimension of the warfare the situation changes. The absence of the clear borders and the independent both state and non-state actors bring challenges for the International Relations theories. Thus, neo-realism struggles to identify the aggressor and the possible victim for the attacks. Moreover, the cyber anarchy requires the new security strategies in the absence of the state actors. When it comes to the constructivism, the theory lacks probably the most concepts for understanding the cyber relations. The basics of the theory lay in identifying state and actors where Westphalia treaty sets their definition. However, the cyber space does not yet have the borders and sovereign states to form the behavioral picture. Liberalism lacks the explanations and understanding of the non-state actors and their behavior in the cyber space. Even together with Westphalia ideas, the theory cannot fully explain the issues occurring in the new dimension.

Thus, the old Westphalia principle plays the crucial role in the international relations theories, their concepts and ideas. However, with the constantly changing characters and under-researched character the treaty cannot fully set the basics for theories to apply their explanations. On the basis of what it is fair to argue that a modernized Westphalian paradigm that is also a more 'customized' for the cyber-world is required to regulate the international relations and create the practical basic for drafting defense strategies.

2.INTERNATIONAL REACTION ON CYBER THREAT

The cyber threat is universal. There is no country absolutely protected from the cyber attack. The states started to implement the new policies and strategies on the cyber security almost immediately after the first cyber attack took place. The IT technologies and Internet development raised the importance of securing the country's cyber space on the national and international levels. The following chapter is divided into two main sections. The first section analyses the reactions and new strategies implementation of the USA and China. These countries considered to be the main and most

powerful states in terms of cyber security, and at the same time, they are probably the most frequent victims cyber attacks wise. The second part discusses the reactions of the smaller states. It represents the case studies of New Zealand and Australia.

2.1. The major players

The USA and China are one of the major players in the international arena. The economies and military capabilities of both states are at the proper level. However, both countries are equally vulnerable when it comes to the cyber threat. Governments of the counties actively work towards the improvement of their defense systems and strategies. The following section discusses the major policy implementations in terms of cyber security and international cooperation undertaken by both states.

2.1.1. Case study: The United States of America

The USA is the key player and hegemon of the modern international system. The country holds the military power along with the economic and political influence over the international community. The USA is a key ally of NATO and the United Nations (UN). However, its cyber space tends to be frequently targeted. There have been numerous cyber attacks of the different kinds and consequences on the USA. Hence, the government develops the defense strategies and preventive methods on both domestic and international level. The following chapter brings up and studies these implementations.

Already in 2008, the Bush's administration prepared the Comprehensive National Cyber Security Initiative aimed to create the secure cyber space of the USA (Gady and Austin 2010, 6). During the following year, the Obama's administration confirmed the cyber security the important issue and added it to the National Security Strategy. Moreover, the National Security Strategy 2010 confirmed for the first time admitted the cyber threat shift from simple non-state cyberterrorism to the state-sponsored activities (Permik 2016, 8). The document states the US intentions to work on forming the sustainable and secure cyber space. In order, to provide the secure environment for international trade, commerce and partnerships within cyber space. The US government also admits the probable consequences of the cyber attack such as loss of human life and serious property damage.

The most recent Cyber Strategy published by the Department of Defence in April 2015 states the three primary missions in terms of providing secure cyber space. They are the following: defending of the US network systems, the national interests against cyber attacks, providing integrated cyber capabilities in order to support military operations (The Department of Defense Cyber Strategy 2015, 4-5). The document proposed the main five goals of the American government cyber security wise. The document proposes the new policy implementations, creating the new institutions and establishing more deep communication between the agencies on a domestic level. What is more important, the fifth main strategic goal identified by the Department of The Defense (2015, 15) is to: "build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability".

The US government priorities the rebuilding cooperation in terms of cyber threat prevention. Along with the strengthening already existing strategies with NATO and its key allies. The US government also stresses out the necessity of improving and in some cases creating the new partnerships in the Middle East and the Asia Pacific region. These are strategically important partners for the USA. First of all, both regions are two greatest growing defense spending markets (Burton 2017,6). Secondly, having such partners in the political arena would increase the overall influence of the USA. But also, it would give an opportunity to shorten NATO's and American's financial expenses in that field. The strategy goes on confirming the necessity of establishing partnerships of networks and system with the above-mentioned regions. What is more, the American government confirms the importance of developing counter cyber threat methods in order to have the protective system from the destructive malware (The Department of Defense Cyber Strategy 2015, 27). Already in 2009, Obama called for the creation of the international environment for cyber security strategy oriented for cooperative actions along with the most technologically developed countries such as Russia and India (Gady and Austin 2010, 2).

The US government also works towards strengthening relations with China. First of all, it is a powerful and influential ally cyber security wise. China's cyber capabilities are strong enough for providing the needed level of help in terms of developing the cyber defense strategy. Moreover, from the strategic perspective, having such a dangerous country as an ally is safer than being enemies with. Especially

when it comes to the cyber war. In 2015 President Obama and Chinese President Xi signed the cyber security agreement. The document confirmed that both countries will no longer sponsor economic espionage in the cyber space, more particularly "the theft of the intellectual property and trade secrets" (Louei 2017). Both countries used to attack each other's cyber space that did not have a positive effect on the political relations between states. However, the agreement aimed to ease the tensions between states and develop strong cooperation cyber space.

Along with building the strategic partnerships with the particular countries, the USA is a member of the Five Eyes Agreement. The members signed the agreement together with the USA are following: New Zealand, the United Kingdom, Australia, Canada and the NATO. According to Dailey (2017, 1), the Five Eyes "is the most enduring and comprehensive intelligence alliance in the world and is uniquely situated to handle the challenges brought by globalization".

The basic aim of the agreement is to provide the collective security on the intelligence institutions level, not directly providing the military support. America's Intelligence agencies community is the largest contributor to the agreement. Such organizations as Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) provide the most help in investigations and detections of the possible attacks. They collect their knowledge and resources between themselves and the intelligence agencies of the other member states. As a result, there is a well-working chain of the data and experiences exchange leading to the increased awareness of the situation in the cyber space. Thus, there is a step forward in term of creating more cooperation on the cyber level undertaken by the USA.

To sum up, the USA is one of the most frequent targets of the cyber attackers. The most recent example is the cyber intervention to the presidential campaign in 2016. The US government officially admitted the existence of the cyber threat to the state security. The numerous steps were made in order to create the strategy as for the domestic and foreign policy. In order to create the sustainable system of the coping with the possible attack in the cyber space. Moreover, the international cooperation and developing partnerships with the foreign states lead the USA towards establishing the well-structured strategy of threat prevention and detection.

2.1.2. Case study: China

China is one of the world's most powerful states in terms of politics and economy. At the same time, the country reached a respected level of development cyber space wise. Thus, the state internationally considered to be a potential cyber-aggressor. China believed to be responsible for the numerous cyber attacks and espionage such as the attack against Google in 2010 and the Indian National Security Council. However, it tends to be frequently attacked. The most recent one hit the country in 2017, the attackers targeted the governmental organizations and schools. The following chapter analyses the reactions and strategic implementations undertook by the Chinese government.

It is important to mention that China represents the different cultural and geographical side of the story. Unlike Western countries, China follows cultural and customs principles even in politics. Thus, the Chinese government does not favor an idea of joint dealing with the threat. As the intervention into the internal affairs and legislations is not accepted. Thus, the country strongly believes in "cyber sovereignty" (Raud 2016,5). China believes that establishing of the national regulations and laws within each state is the better solution than creating one single law. One more challenging thing about the state is its difficult relations with the USA. Despite the cyber agreement of 2015 mentioned above, there are problems in finding the ultimatum and understanding in the overall between two states. The Western ideology highly contradicts to what the Chinese people tend to believe.

However, despite the facts mentioned above the Chinese government confirms the existence of the cyber space and the need to establishing the new strategy of dealing with it. The document 27 established already in 2003 was a breakthrough in Chinese politics cyber security wise. According to Raud (2016,11), it established the implantations to the cyber security policies and strategies, as well as the mechanism of the national recovery and e-government plans. China also supports the UN framework on cyber space security and the necessity of establishing the universal approach towards the attack of that kind. Later in 2012, the Chinese government published "The State Council vigorously promotes normalization development and offers several opinions on conscientiously protecting information security" (translation from Chinese, Chen 2010). The document confirmed that the goals set before not yet met. However, it argues for the strengthening the existing networks cyber protection wise; strengthening of the governmental systems against the cyber attacks; increasing protection of the industrial systems and infrastructures; and increasing protection of the citizen's personal data (Giles and Hagestad 2013). The National Network Emergency Response Technical

Team (CNCERT) established in 2002 is a non-governmental organization meant to provide the technical assistance in terms of detecting the malicious systems (Raud 2016, 16). These are the short summary of the most remarkable attempts of China in order to regulate the cyber security on the national level.

However, considering the scale of the threat China confirms the need of creating more international partners in order to have more secure national cyber space. ASEAN states along with China, Russia, the US, Japan, the Republic of Korea and Australia signed an agreement acknowledging (ASEAN Regional Forum Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space 2006):

> … importance of a national framework for cooperation and collaboration in addressing criminal, including terrorist, misuse of cyber space and encourage the formulation of such a framework.

The remarkable step forward towards building the new international partnerships was joining the Shanghai Cooperation Organization (SCO). The heads of the organization confirmed that they will work together towards providing the secure cyber space. Later, in 2009, China along with the SCO members signed the first treaty on Informational Security, confirming the development of the new international laws and regulations cyber threat wise (Osula and Rõigas 2016, 148). *The White Paper* published in 2010 also confirmed the development of the international cooperation of China with the foreign states. The document confirmed the intentional of the state to spread the internet all over the country. But at the same work together with the other states in order to provide the security environment for the internet (White Paper – The Internet in China 2010). One more important step towards establishing the international cooperation with the foreign states was in 2015. Russian and China signed a non-aggression agreement confirming that both parties will no longer undertake attempts of the cyber attack and interfere affairs of the different state (Osula and Rõigas 2016, 148).

To sum up, China has its own views on politics and cooperation. However, the new kind of threat requires the new methods of dealing with it. Thus, China made a breakthrough for its own policies in terms of establishing partnerships with the foreign states. And joining the international organizations in order to work on the new international regulations and legislation. The country now plays an

important role in joint work towards establishment of the collective cooperation even with such states as the USA.

2.2. The smaller states

Today the world's politics mostly controlled by the bigger powers such as the USA, China and Russia. These states can affect the politics and set the directions of political development. However, in the cyber space, every country is equally predisposed to the threat. Thus, it is necessary to have a look at the political implementations and reactions of the smaller states such as New Zealand and Estonia. In order to get the better overview of the cyber security capabilities in the overall. The following section analyses the cyber security strategies development of New Zealand and Estonia, and analysis their intentions for international cooperation.

2.2.1. Case study: New Zealand

Geographically, New Zealand is a remote country from the main political arena. This influenced the foreign policies directions of the country. Firstly, its alliance with the Great Britain during the two World Wars. After the war Britain lost its political influence, New Zealand turned to the USA aiming for support and security. The cyber space of the country tends to be frequently attacked. New Zealand's government is concerned if the state is capable to defend itself in today's highly globalized world. The following chapter analyzing the cyber regulation and attacks prevention attempt undertaken by New Zealand.

Interestingly enough, New Zealand was once – before the geostrategic 'shakeup' in 1980s – an active member of the Security Treaty of Australia, New Zealand and the USA (ANZUS). The alliance – still in existence with the 'NZ' in its abbreviation but without New Zealand in it – aimed to provide the collective security similar to NATO. It is important to mention that New Zealand was a founding member of the UN and spoke for the role of the smaller countries later after the organization formation (Burton 2017, 225). Coming back to the ANZUS, the relations with the core ally – the USA worsened due to the nuclear question. However, the country remained within the organization New Zealand does not see the high strategic importance of its membership.

When it comes to the cyber security, the first to be mentioned is the National Cyber Security Strategy. The document confirmed that the country is not immune to the cyber threat and the relevant measures required to secure the national cyber space (New Zealand's Cyber Security Strategy 2011,3). Moreover, the Action Plan (New Zealand's Cyber Security Strategy 2016) confirmed four main principles, they state: Partnerships are essential; Economic growth is enabled; National security is upheld; Human rights are protected online. The document confirms the necessity of creating the partnerships both on the domestic level within enterprises and on the international arena. Moreover, the goal is to be capable to detect and prevent the cyber attack on the technological level. What is more, the private companies and individuals should be aware of the threat and the possible protective measures.

New Zealand is also the member of the National Cyber Security Centre (NSCS), the umbrella concept for an alliance between intelligence agencies of New Zealand, the USA, the UK, Australia, Canada and Australia (Burton 2017, 229). The NSCS aimed to provide assistance on protecting the computer and internet systems of the member states. Moreover, the country joined the NATO's Individual Partnership Cooperation programme (Partnership arrangement signed with NATO 2012). That aims to provide a constant data and knowledge sharing among the member's cyber security wise. The country also joined the Computer Emergency Response Team (CERT) as a part of the Cyber Security Strategy 2015 (CERT NZ About us). First of all, CERT works towards the threat detection by gathering the information from all its members and analyses the gathered data on the professional level. Moreover, the organization allows the simple individual report of a problem or possible cyber attack. And finally, the CERT is able to provide a prompt and effective response to the cyber-threat.

To sum up, New Zealand historically depended on the allies and its foreign policies highly deepened on it. However, when it comes to the cyber space, New Zealand creates its counter cyber threat policies independently. What is proved with the Cyber Security Strategies and actions plan. However, the cyber threat is impossible to be handled only by one country, and the New Zealand Government seem to understand it. Thus, there is a cooperation on the international level of a different kind, from the cooperation on the overall governmental level to the intelligence agencies data exchange.

2.2.2. Case study: Estonia

Estonia is the remarkable state cyber security wise. It is the first state that was targeted with the cyber attack. Unfortunately, at the moment of the attack, the international political society was not educated about that kind of attacks. The country was vulnerable and was to cope with the situation on its own. Thus, it is interesting to have a look at what has changed since the attack in terms of the Estonian cyber security strategies. The following chapter analyses the policy implementations cyber security wise.

According to the Cyber Security strategy 2008 (27), Estonia follows four main Strategic goals, they are: establishment of a multilevel system of security measures; expanding Estonia's expertise in and awareness of information security; adopting an appropriate regulatory framework to support the secure and extensive use of information systems; consolidating Estonia's position as one of the leading countries in international co-operative efforts to ensure cyber security. Thus, Estonia reacted promptly. After the attack, the country established close cooperation with the EU. As a result, the IT center was established in Estonia in order to develop the preventive and identification measures in terms of cyber security (Crandall 2014, 37). The attack revealed the necessity of cooperation between first of all member-states of the EU. Secondly, the cyber attack on Estonia made it clear that the old legislation does not apply to the new threat. Thus, the possible reaction of the countries is not regulated and therefore can be illogical.

The NATO's article 5 was criticized and put under the discussion. However, NATO and Estonia started more close cooperation. NATO started with the establishment of the Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn, the Estonian Capital city. That can be considered the breakthrough of the Estonian Cyber Security policies. The center works on both technical and legal aspects. That gives a number of advantages to Estonia. Moreover, Estonia established the volunteer organization Cyber Defense League (CDL) aiming to protect the e-life of the country (Cardash, Cilluffo and Ottis 2013, 779). The main task is to spread the cyber awareness within the society and to improve the IT skills in order to be able to trigger the attack. The CDL also works closely with CCD COE (Crandall 2014,39). Thus, the experts working for CDL have the full range of capabilities and knowledge in order to provide the country with the valuable solutions cyber security wise.

Moreover, the country seeks for strategic parents not only in Europe and America but also in the Middle East and Southeast Asia (Annual Cyber Security Assessment 2017 Estonian Information System Authority, 48). The cooperation lies in the annual meetings of the experts in order to maximize the overall situation in the cyber space, to evaluate the threat level and set the possible solutions. One of the latest meetings was the digital summit in Tallinn in spring 2017. One of the conclusions made during the summit was about the necessity of building the common European cyber space, providing security together by providing mutual technical and theoretical support. The document confirmed that Europe: "must improve our national and joint preparedness, crisis-management capabilities as well as incident reporting and analysis" ('Conclusions of the Prime Minister of Estonia Jüri Ratas after the Tallinn Digital Summit' 2017).

Estonia is highly developed country in terms of e-industry. Thus, the government copes with the data and personal information protection on the daily basis. Thus, already in 2008 Estonian Cyber Security Strategy confirmed the need for increasing the competence in cyber space. Moreover, Estonia established the governmental agency, the Information System Authority (RIA), which aims to protect and improve the nation's digital society. The agency works on developing the response methods and regulations of the cyber attacks. Along with working on the internal level and cooperating with the agencies and instructions on improving the security of the Estonian cyber space. The RIA improves its partnerships with the NATO and EU in order to be able to assist its own nation in case of the attack. Also, to share the knowledge and gain some new techniques and skills from the partners. Moreover, the RIA cooperates with the Digital Five (D5) in order to provide "secure digital identification solutions" (Annual Cyber Security Assessment 2017, 49).

To sum up, Estonia is a relatively small state on the political map of the world. However, due to the fact that it was the first nation-state officially experienced the cyber attack, the country actively works on securing its cyber space. Estonia created a number of governmental and non-governmental organization in order to develop the more advanced cyber security strategy on the national level. Moreover, considering the scale of the danger carried by the cyber space, Estonia actively cooperates on the international level. Thus, the country has close relations with NATO cyber security

development wise. Moreover, the state works together with the EU member states on providing valuable solutions and regulation in order to control the cyber threat.

2.3. Case Study: NATO

When it comes to the NATO, the organization is actively trying to adjust the existing policies and strategies to the new kind of threat. According to Burton (2015, 304), the cyber threat has provoked the institutional change within NATO. The 9/11 attack played the decisive role counterterrorism strategies wise. The attack on Estonia and China raised concerns about the cyber security among the members. Moreover, the active actions of the world's leaders such as China and Russia within the cyber space and the growing number of the attacks add more complexity to the term. The following chapter discusses the NATO's strategic implementations in cyber space and its overall view on international cooperation defense wise.

One of the first steps towards building the cyber security strategy was establishing of the NATO CCDCOE in the Estonian capital. The office's main responsibility is to be policies and strategies development advisor. The organization made some evolutional changes after the first serious cyber attacks. The Strategic Concept of 2010 confirmed that the main focused for now is cyber security. The document claimed that the cyber threat is not only national today, but it reached the global level. NATO's Strategic Concept (2010, 11) states that frequency of the cyber attacks is increasing, and it can reach a threshold that potentially threatens the national and Euro-Atlantic prosperity, security and stability.

Later in 2011 NATO published Cyber Defense Policy. The document argued for the necessity of establishing the minimum requirements for the cyber defense on both national and international levels. The main idea behind was to create an integrated system of NATO and national governments cooperation in order to provide the pragmatic response to cyber attacks (Burton 2015, 308). One year later the Rapid Reaction Team was formed (RRT). The team consists of 6 competent experts in cyber security capable to assist the national governments in case of the attack (NATO Rapid Reaction Team to fight cyber attack 2012). Thus, in case of the potential attack, any NATO's ally will be able to ask

for help. However, even non-NATO countries will be able to ask for an additional assistance from the RRT, the North Atlantic Council will make decisions in this case (NATO Rapid Reaction Team to fight cyber attack 2012). Finally, in 2014 during the Cardiff Summit, the NATO members equalized cyber attacks with the kinetic attacks. Thus, the Article 5 now applies also to the conflict in cyber space and oblige allies for a collective defense measure in that sense (Burton 2015, 308).

However, the organization clearly understand with the existing list of allies the global cyber threat may be difficult to foster. The international cooperation of the new kind is needed in order to be able to build the counter cyber attack strategies and technologies for the global usage. The innovative approach towards cooperation is now one of the core tasks of NATO. First of all, it applies to the building and developing strategic relations with the Asia-Pacific states. The novel for the international relations concept of the cooperative security with the main five global partners (Chaban et.al. 2017, 2). They are Australia, Mongolia, South Korea, Japan and New Zealand. The mentioned countries probably do not see NATO as its core ally and partner in politics. However, the majority of the countries contributed to the NATO military and intelligence wise. For example, the organization's operations in Afghanistan and Iraq. Thus, according to Burton (2017, 12) who cited an official from the Summit in Brussels 2015, it is logically that NATO will be ready to help any of these countries in case of the crisis by the military, political and financial means. Moreover, the organization provided the countries with the understanding that their help before is valuable for the members.

The strategic partnership with Japan is worth mentioning separately. The current situation with China and Russia political influence on the political arena tends to improve the cooperation between countries with the complicated past relations. Japan is highly capable in cyber operation, therefore is a valuable partner cyber security wise. Along with the financial benefits of having such an ally as NATO, the security and defense cooperation is valuable for Japan. The cooperation between the major NATO ally- the USA and Japan may be challenging. However, Schriver and Ma (14) believes that:

> (…) the U.S. may be able to foster deeper Japan - NATO cooperation by supporting Japan's participation in NATO activities, particularly those where U.S. takes a prominent leadership role, to build confidence and amity between the two parties for future collaboration.

As a result, Japan officially confirmed its membership with the CCDCOE in Tallinn (Japan to Join the NATO Cooperative Cyber Defense Centre of Excellence in Tallinn, 2018). However, it is important to mention that NATO tends to look for more strategic cooperation in cyber security not only in Asia Pacific region but also with the European Union. Secretary Clinton (2012, 10) mentioned during the North Atlantic Council meeting "our pivot to Asia is not a pivot away from Europe. On the contrary, we want Europe to engage more in Asia, along with us to see the region not only as a market, but as a focus of common strategic engagement". Thus, NATO tries to improve cooperation between the Asia Pacific regions and the EU in order to reach the mutual security goal. The existing relations with the EU are quite satisfactory when it comes to cooperative defense strategy. Therefore, the organization along with the EU member states currently work on improving the existing counter methods against the hybrid attacks (the cyber attack is one of such threats). The existence of the Estonian CCDCOE is on the examples demonstrating the developing cyber security strategy between NATO and the EU.

To sum up, NATO as one the most powerful military wise international organizations realizes its role in creating the secure cyber space. The organization works towards creating evolutionally new memberships with the Asia Pacific countries. That is quite challenging considering the past relations between NATO's core ally, the USA, and some states like Japan. The global threat unites the states. As now the geographically located unit faces the digital threat, and there is a question if it is capable to respond to such kind of attack (Burton 2015, 298). Thus, there are quite noticeable evidences demonstrating the growing cooperation and strategy development cyber security wise.

3.A POST-WESTPHALIAN CYBER ERA?

The previous chapter discussed the reactions of some countries on the cyber threat. It is important to mention that the author pointed out the main strategic answers the discussed countries have. However, the mentioned previously countries are not the only states interested in securing their national and global cyber space. The states try to adjust their existing policies and develop the new strategies in order to be protected from the cyber threat. These attempts fairly can be considered the evidence that the existing world order and its principles are outdated. And the changes along with the new world order model is coming. The following chapter tries to prove that the Westphalian principles are being shifted towards the new cyber-treaty.

The novel nature of the cyber threat requires the new methods of confronting it. First of all, the new dimension of the conflict has the number of absolutely new characteristics. For example, there are no national borders in the cyber space. Moreover, the notion of 'power' is different. It is difficult to say that there is one world power in the cyber space capable of controlling the situation. All state and non-state actors are equally vulnerable. Moreover, the novelty of the cyberwar is challenging legislations and regulations wise. The states just start adjusting the existing laws. And their judgement about the cyber threat in the overall. Thus, some scholars argue that cyber space is moving away from the Western power and control (Demchak 2016, 49). Some believe that the current counter cyber attacks methods are not effective (Shackelford 2013,1279). Therefore, the Western states try to gather their influence and capabilities together with the minor states in order to build the defensive mechanisms. The situation in the world now can be easily compared with the one during the World War I. There was a conflict of all between all. However, the outcome was surprisingly positive. The creation of the League of Nations is an example for that. Thus, the contemporary state of affairs in international relations may signalize the beginning of the new era.

The states need to develop and improve the existing regulations and legislation. Moreover, there is a need for the innovative approach and the ability to adapt due to the nature of the cyber threat. The

global threat needs the cooperative solution. Bebber (2017,429) believes that the alliances will have more advantages in terms of confronting the cyber-conflict. The argument behind is that the smaller states will get more advantages by cooperating with the bigger states. And the bigger states will enjoy the knowledge and practices exchange. Hughes (2010, 523) also considers cooperation as an advantage for the smaller states looking for "gaining an asymmetric edge" of the contemporary battlefield. According to the Council of Europe Convention of Cyber-Crime (2001,2), there is a need for cooperation between states and the private firms in order to protect the society and develop the information technologies capable of combating the cyber threat. Bebber (2017,429), also believes that the command and control techniques require cooperation. In order to be able to control the situation in the cyber space the leader is needed. However, considering the list of countries (such as the USA and Russia) and non-states actors (such as ISIS and Hezbollah) who prefer the defensive cyber defense techniques it is reasonable to say that there will hardly be only one leader. That is an unusual fact for the methods for world peacekeeping. The example of the USA led war on terror proved that only one state may be not fully capable of defending the global threat (Czosseck and Hughes 2009, 115). But the opposite can negatively influence the overall situation.

The cyber - threat prevention is challenging for the modern state. Handling of the problem requires not only legislative foundations but also strategic and technical solutions. Scholars today tend to believe that the existing world order principles in the overall will change under the cyber conflict pressure. The majority of them question the Westphalian Treaty and its legitimacy in the modern technologically changed world. According to Demchak (2016, 50), governments and major international organizations are creating "Cyber Westphalia", of laws and regulations more concentrated on the new border's establishment and working on international cooperation.

Westphalia treaty formed the existing world structure. First, it established the clear national borders and understanding of their sovereignty. Thus, in the event of the aggression, each state can provide security and stability for its citizens by defending the national borders. The balance of power was one of the main outcomes of the treaty. As if there are stronger states dominating over the weaker ones the stability on the international level is difficult to achieve. Moreover, the clearly designated borders positively affected the social and economic development. What is more, Westphalia was a turning

point for providing the collective security among the state-actors and core tasks for the International Relations.

When it comes to the cyber space and the challenging character of its threat, the modern states are trying to establish something new but similar to Westphalian principles. The first discussions on how to secure the citizens from the digital threat started early in the beginning of the contemporary age. However, the greater changes followed the real cases such as Stuxnet and cyber attack against Estonia. One of the main responsibilities of the government is providing the national security. Therefore, defense of the national borders, the countries actively started to work on the cyber security strategies and methods of combating the cyber-threat. According to Nye (2010, 15), the states tend to seek for extending their cyber-sovereignty and develop the technical means for that. The scholar also compares the cyber space to the common pool resources. Ostrom and Burger (1998, 280) argue the solely solution for the problems connected to the pool resources is not efficient in all cases. Thus, it is fair to believe that the cyber threat needs the cooperative solution. The states' partnerships and collective security.

The examples discussed before in the thesis prove that the states from bigger to smaller understand it and try to go for more concrete cooperation. The cyber partnership is a novel concept, so the techniques and principles apply. The main problem of the cyber space is its openness. Thus, the modern governments work on establishing the borders and sovereignty within the new dimension. Same as the states worked before establishing the Westphalian Peace. According to Scassa and Currie (2011, 89), the fact that the internet is borderless changes the overall behavior of the states:

> (…) states are faced with the need to regulate conduct or subject matter in contexts where the territorial nexus is only partial and, in some cases, uncertain. This immediately represents a challenge to the Westphalian model of exclusive territorial state sovereignty under international law.

Thus, the cyber-threat makes the governments re-establish the national borders and legally confirm them. Moreover, the new international agreements on cooperation and technical support among state and non-state actors started their slow but prompt development. The balance of powers in cyber space is a little more challenging point to work on. As was discussed before, anyone who has the internet connection can attack not only individuals but corporations and nation states. Thus, each member of

the cyber space is equally vulnerable. However, states actively work on improving their IT industries. The surprising fact is that geographically smaller states tend to be more proactive and efficient in that terms than the bigger states. Thus, the cyber space is the new and challenging dimension that already changed the world political interface. It positively affected and negatively affected the society. Even though the cyber threat challenged the governments, it also positively affected on the cooperation understanding between states. Westphalia treaty most likely to work as the basis for the treaty that will regulate the word of cyber space. Thus, it is fair to say that the post-Westphalian era does exist and indeed affects the world order.

CONCLUSION

Arguably, the Internet and the Internet-related developments have irreversibly changed the world. It made the life of society easier and more efficient. However, along with the positive side of the changes, the new type of threat appeared. The cyber space slowly turned from the super-fast data exchange platform to a battlefield. The targets of the cyber attack also revolutionized comparing to the previous year's victims. The hackers targeted the individual computers for fun or minor economic benefit. With the advanced development of the technologies the attackers changed the priories. Social sectors such hospitals and schools, private firms, bug corporations and even nation-states now being targeted. This paper confirmed that the prime reason for such a situation is the openness of the cyber space. There are no specific restrictions for the identity of the cyber society participant as if any individual, state and non-state actor with the internet access can join. Moreover, the nature of the cyber space makes it easy for the attacker to hide its real identity and destination. The cyber attack is difficult to foresee and thus to prevent. The new phenomenon is challenging for the politics of the XXI century. Thus, the theories of the international relations struggle to explain and analyze the cyber space and issues occurring there.

In the context of this research work, a discussion on the main theories of international relations was offered to find a proper framework for the debate on the issue. The neo-realist can explain the intentions behind the cyber war. As the world tends to have anarchic nature, thus no one can be sure that the neighboring country will not conduct the war. However, the theory cannot explain if the cyber space can have hegemons and what kind of power should they have. Liberals in their turn, manage to advice on the conflict prevention and detection methods. However, the theory may not provide the full picture of the situation due to the novelty of the cyber space as the warfare dimension. Constructivism most probably is the most suitable theory that can give more clear understanding of the cyber conflict. However, as it is mostly based on the identity and ideology notions. The uniqueness of the cyber space it may be challenging for constructivist to identify the ideas and norms.

The paper also showed the main results of the foreign policies development towards the cyber security form the different perspectives. The USA was one of the first countries to confirm the cyber threat to be the serious risk for the national security. The American government published numerous national cyber security strategies. Which confirmed the need for the international cooperation in order to achieve the peace in the new dimension. Despite its cultural and ideological aspects China decided to join the global movement for the partnership development. The state values the cooperation cyber security strategy wise between governments. Thus, it is fair to say that the major political players not only realize the need for the collective defense against the global threat. But also take proactive actions and indeed build partnerships. When it comes to smaller states like Estonia and New Zealand, both states undertake major attempts in order to build the secure national cyber space. As for Estonia, for example, the state constantly develops its IT infrastructure and works on developing more secure technologies cyber threat wise. Both countries value international cooperation and work for it, look for more options and opportunities in that sense. NATO as one of the most powerful international organization most actively develops its cyber security strategies. The organization develop cooperation between its allies, but also with the evolutionally new partners like the Asia-Pacific states.

The research proves that the current world order and principles are changing. The chosen method helped to show evidences for the re-establishing the nation borders considering the new dimension. The new international legislation and norms are necessary for stabilizing uncertainty of the cyber security. Thus, the new updated version of the Westphalia treaty is needed. However, due to complexity and under researched nature of the concept it is difficult to provide single evidence to confirm the claim. However, there are already signs that states do work on the re-establishing ideas mentioned in the treaty. And indeed, the cyber-Westphalia will take place soon replacing the predecessor and bringing the evolutionary aspects to the world order principles. The topic is worth conducting further research. The author suggests the young scholars and researched to have a deeper look on the international treaties on common cyber security and their results. Moreover, the deeper focus on legislative perspective of the cyberwar, jus in bello and jus post bellum.

LIST OF REFERENCES

10 Steps to Cyber Security. (2012). Executive Companion. CESG. The Information Security Arm of GCHQ, 3. Accessible: http://www.smartprotect.eu/resources/report1.pdf, 11 March 2018.

Annual Cyber Security Assessment 2017 Estonian Information System Authority. (2017). Republic of Estonia Information System Authority, 48-49. Accessible: https://www.ria.ee/public/Kuberturvalisus/RIA_CSA_2017.PDF, 2 April 2018.

ASEAN REGIONAL FORUM STATEMENT ON COOPERATION IN FIGHTING CYBER ATTACK AND TERRORIST MISUSE OF CYBER SPACE (2006). Ministry of Foreign Affairs of Japan website. Accessible: http://www.mofa.go.jp/region/asia-paci/asean/conference/arf/state0607-3.html, 1 April 2018.

Bebber, R. (2017). Cyber power and cyber effectiveness: An analytic framework. Cooperative Strategy, 429. Accessible: https://doi.org/10.1080/01495933.2017.1379833, 4 April 2018.

Bryant, R. (2001). *What Kind of Space is Cyber space?* Minerva - An Internet Journal of Philosophy 5, 139. Accessible: http://minerva.mic.ul.ie/vol5/cyber space.pdf, 11 March 2018.

Burchill, S. (2005). Theories of International Relations.3 edition. New York: Palgrave Macmillan, 60.

Burton, J. (2015). NATO's cyber defence: strategic challenges and institutional adaptation. Defence Studies. Vol. 15, No. 4, 298-308. Accessible: https://doi.org/10.1080/14702436.2015.1108108, 31 March 2018.

Burton, J. (2017). NATO's "Global Partners" in Asia: Shifting Strategic Narratives. Asian Security,6-12. Accessible: http://dx.doi.org/10.1080/14799855.2017.1361728, 22 March 2018.

Burton, J. (2017). Small states and cyber security. Political Science, 225. Accessible: https://doi.org/10.1177/0032318713508491, 1 April 2018.

Cardash.L.S., Cilluffo.J.F., Ottis.R. (2013). Estonia's Cyber Defence League: A Model for the United States? Studies in Conflict & Terrorism, 779. Accessible: https://www.tandfonline.com/doi/pdf/10.1080/1057610X.2013.813273?needAccess=true, 1 April 2018.

CERT NZ. About US. Accessible: https://www.cert.govt.nz/about/about-us/, 1 April 2018.

Chaban. N., Bacon. P., Burton. J., Vernygora. V. (2017). NATO Global Perceptions – Views from the Asia- Pacific Region. Asian Security, 2. Accessible: http://dx.doi.org/10.1080/14799855.2017.1361726, 1 April 2018.

Chen, W. (2010). Concerning the Development and Administration of Our Country's Internet. Human

Clausewitz, C. V. (1976). *On War*. Princeton: Princeton University Press, 90.

Clinton, H. (2012). THE TRANSATLANTIC PARTNERSHIP: A STATESMAN'S FORUM WITH SECRETARY OF STATE HILLARY CLINTON. THE BROOKINGS INSTITUTION, 10. Accessible: https://www.brookings.edu/wp-content/uploads/2012/11/20121129_transatlantic_clinton.pdf, 1 April 2018.

Conclusions of the Prime Minister of Estonia Jüri Ratas after the Tallinn Digital Summit. (2017). Official website EU2017.ee. Accessible: https://www.eu2017.ee/news/insights/conclusions-after-tallinn-digital-summit, 2 April 2018.

CONVENTION ON CYBERCRIME. (2010). Council of Europe, 2. Accessible: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf, 4 April 2018.

Couzigou, I. (2018). Securing cyber space: the obligation of States to prevent harmful international cyber operations. International Review of Law, Computers & Technology, 41. Accessible: https://doi.org/10.1080/13600869.2018.1417763, 11 April 2018.

Crandall, M. (2014). Soft Security Threats and Small States: the Case of Estonia. Defence Studies, 37-39. Accessible: https://doi.org/10.1080/14702436.2014.890334. 1 April 2018.

Cyber Security Strategy. (2008). Ministry of Defence Estonia, 27. Accessible: https://www.unodc.org/res/cld/lessons-learned/cyber-security-strategy_html/Cyber_Security_Strategy_Estonia.pdf, 2 April 2018.

Czosseck. C., Geers. K,. Hughes.R. (2009). The Virtual Battlefield: Perspectives on Cyber Warfare. Amsterdam: IOS Press BV. Vol.3., 115.

Daile, J. (2017). The Intelligence Club: A Comparative Look at Five Eyes. Journal of Political Sciences & Public Affairs, 1. Accessible: https://www.omicsonline.org/open-access/the-intelligence-club-a-comparative-look-at-five-eyes-2332-0761-1000261.pdf, 22 March 2018.

Demchak, C. C. (2016). Uncivil and post-western cyber westphalia: Changing interstate power relations of the cybered age. THE CYBER DEFENSE REVIEW, 49 - 50. Accessible: http://digital-library.usma.edu/cdm/ref/collection/p16919coll8/id/11, 4 April 2018.

Demchak. C. C., Dombrowski. P. J. (2013). *Cyber Westphalia Asserting State Prerogatives in Cyber space.* Georgetown Journal of International Affairs. International Engagement on Cyber III:

State Building on a New Frontier, 30. Accessible: http://www.jstor.org/stable/43134320, 10 March 2018.

Demchak. C. C., Dombrowski. P. J. (2011). *Rise of a Cybered Westphalian Age: The Coming Decades*. The Global Politics of Science and Technology. Vol.1. Global Power Shift, 32-33. Accessible: http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-05_Issue-1/Demchak-Dombrowski.pdf, 21 February 2018.

European Commission, High Representative of the Union. (2013). - JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyber space. I Final, 3. Accessible: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN, 26 February 2018.

Gady. F., Austin. G. (2010). Russia, The United States, And Cyber Diplomacy. Opening the Doors. New York: The EastWest Institute, 2-6.

Geers, K. (2011). *Strategic Cyber Security*. Tallinn: CCD COE Publication, 97.

Giles. K., Hagestad. W. (2013). Divided by a Common Language: Cyber De nitions in Chinese, Russian and English. 5th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallinn.

Glaser. L. C., Kaufmann. C. (1998). What is the offense-defense balance and can we measure it? (Offense, Defense, and International Politics). International Security. V.22. №.4, 7. Accessible: https://web.stanford.edu/class/polisci211z/2.1/Glaser%20%26%20Kaufmann%20IS%201988.pdf, 21 March 2018.

Highes, R. (2010). A treaty for cyber space. International Affairs. Vol. 86, 523-535.

Ho, D. (2006). *The focus group interview: Rising the challenge in qualitative research methodology*. Australian Review of Applied Linguistics, Vol.29 №1, 11. Accessible: https://benjamins.com/#catalog/journals/aral.29.1.03ho/details, 27 February 2018.

Isnarti, R. (2016). A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. Andalas Journal of International Studies. Vol 5. No 2, 155-161.

Japan to Join the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn. (2018). CCDCOE official website. Accessible: https://ccdcoe.org/japan-join-nato-cooperative-cyber-defence-centre-excellence-tallinn.html, 1 April 2018.

Kozlowsi, A. (2014). *COMPARATIVE ANALYSIS OF CYBERATTACKS ON ESTONIA, GEORGIA AND KYRGYZSTAN*. Special Edition. European Scientific Journal. p.238. Accessible: http://www.eujournal.org/index.php/esj/article/viewFile/2941/2770, 26 February 2018.

Krasner, S. D. (1995). Compromising Westphalia. International Security, Vol. 20, No.3,123. Accessible: http://www.jstor.org/stable/2539141?read-now=1&loggedin=true&seq=8#page_scan_tab_contents, 11 May 2018.

Krasner, D. S. (2011). Rethinking the sovereign state model. Review of International Studies Vol.27, 22. Accessible: http://vanity.dss.ucdavis.edu/~maoz/krasner2001.pdf, 11 May 2018.

Liff, P. A. (2012). *Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War*. Journal of Strategic Studies. Vol. 35, No. 3,404. Accessible: https://www.tandfonline.com/doi/pdf/10.1080/01402390.2012.663252?needAccess=true, 11 March 2018.

Louie, C. (2017). U.S. - China Cyber security Cooperation. The Henry M. Jackson school of International Studies. The University of Washington. Accessible: https://jsis.washington.edu/news/u-s-china-cyber security-cooperation/ , 27 March 2018.

NATO Rapid Reaction Team to fight cyber attack. (2012). NATO official webpage. Accessible: https://www.nato.int/cps/en/natolive/news_85161.htm, 31 March 2018.

Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches*. 9th Edition. Boston: Pearson, 42.

New Zealand's Cyber Security Strategy. (2011). New Zealand Government, 3. Accessible: https://webcache.googleusercontent.com/search?q=cache:GFWivkDmwY0J:https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/new-zealands-cyber-security-strategy+&cd=4&hl=en&ct=clnk&gl=ee&client=safari, 1 April 2018.

New Zealand's Cyber Security Strategy. (2016). Action Plan Annual Report. Accessible: https://www.dpmc.govt.nz/sites/default/files/2017-06/nzcss-action-plan-annual-report-2016.pdf, 1 April 2018.

Nye, S. J. (2010). Cyber Power. Harvard Kennedy School. Belfer Center for Science and International Affairs, 15. Accessible: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf, 7 April 2018.

Nye, S. J. (2012). Cyber War and Peace. Accessible: https://www.project-syndicate.org/commentary/cyber-war-and-peace?barrier=accessreg, 7 April 2018.

Nye. S. J., Welch. A. D. (2013). *Understanding Global Conflict and Cooperation. An Introduction to The Theory And History.* – New Jersey: Pearson Education Inc, 331-338.

Ostrom. E., Burger. J., Fleld. B. C., Norgaard. B. R., Pollcansky. D. (1999). Revisiting the Commons: Local Lessons, Global Challenges. SCIENCE'S COMPASS. Review, 280. Accessible: http://science.sciencemag.org/content/sci/284/5412/278.full.pdf, 7 April 2018.

Osula. A., Rõigas. H. (2016). International Cyber Norms. Legal, Policy & Industry Perspectives. Tallinn: CCD COE Publication, 148.

Partnership arrangement signed with NATO. (2012). The official website of the New Zealand Government. Accessible: https://www.beehive.govt.nz/release/partnership-arrangement-signed-nato, 1 April 2018.

Permik. P., Wojtkowiak. J., Verschoor-Kirss. A. (2016). National Cyber Security Organisation: UNITED STATES. Tallinn: CCD COE Publication, 8.

Raud, M. (2016). China and Cyber: Attitudes, Strategies, Organisation. Tallinn: CCD COE Publication, 5-16.

Rid, T. (2013) *Cyber War Will Not Take Place.* 1st Edition. New York: Oxford University Press, 10.

Rights In China. Accessible: https://www.hrichina.org/en/content/3241, 1 April 2018.

Scassa. T., Currie.J. R. (2011). NEW FIRST PRINCIPLES? ASSESSING THE INTERNET'S CHALLENGES TO JURISDICTION. Georgetown Journal of International Law, Vol. 42, 89. Accessible: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2116364. 7 April 2018.

Schriver. R., Ma. T. The Next Steps in Japan – NATO Cooperation. Project 2049 Institute, 14. Accessible: https://project2049.net/documents/next_steps_in_japan_nato_cooperation_schriver_ma.pdf, 1 April 2018.

Shackelford, J. S. (2013). Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance. American University Law Review. Volume 62. Issue 5. Article 6, 1279.

Sigholm. J. NON-STATE ACTORS IN CYBER SPACE OPERATIONS, 2. Accessible: https://www.google.ee/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjMrZSK9vDZAhVKqaQKHWA3C7sQFgg4MAE&url=https%3A%2F%2Fjournal.fi%2Fjms%2Farticle%2Fview%2F7609%2Fpdf_1&usg=AOvVaw0i_TIRoMOEE-up_fBsK6ui, 16 March 2018.

Strategic Concept. (2010). NATO, 11. Available: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf, 31 March 2018.

THE DEPARTMENT OF DEFENSE CYBER STRATEGY. (2015), 4-27. Accessible: https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, 22 March 2018.

Theohary, A. C. (2015). *Information Warfare: Cyberattacks on Sony.* CRS Insights (IN10218). Accessible: https://fas.org/sgp/crs/misc/IN10218.pdf, 11 March 2018.

Tuthill, P. D. (2012). Reimagining Waltz in a Digital World: Neorealism in the Analysis of Cyber Security Threats and Policy. University of Kent, 20. Accessible: http://paultuthill.com/dissertation/Dissertation_Tuthill.pdf, 10 May 2018.

Valeriano. B., Maness. C. R. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. Journal of Peace Research. Vol. 51(3), 348. Accessible: http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/cyber_dyanamics_jpr_51-3.pdf, 15 March 2018.

Waltz, K. N. (1990). REALIST THOUGHT AND NEOREALIST THEORY. Journal of International Affairs. Vol. 44, No. 1, Theory, Values And Practice In International Relations: Essays In Honor Of William T.R. Fox, 29.

White Paper - The Internet in China (2010). The Information Office of the State Council of the People's Republic of China. Accessible: https://www.sbs.ox.ac.uk/cyber security-capacity/system/files/Internet%20in%20China.pdf, 1 April 2018.