TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Department of Law

Lia Nodarishvili

Is Cyberspace a New War Domain?

Bachelor's Thesis

Programme International Relations

Supervisor: Holger Mölder, PhD

Tallinn 2018

I hereby declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
has been properly referenced and the same paper
has not been previously presented for grading.
The document length is 10694 words from the introduction to the end of conclusion.

Lia Nodarishvili …………………………………….
(signature, date)
Student Code: 156111TASB
Student e-mail address: likanodarishvili@gmail.com

Supervisor: Holger Mölder, PhD:
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 thesis is to provide conceptual framework in controversial probability of cyberspace establishing itself as the 5th domain of the war. With the advent of information technologies nation-states started widely utilizing politically motivated cyber offences on adversaries. By analyzing the concept of war and conducted cyberattacks, thesis asserts that cyberspace is not an independent war domain, but an environment which facilitates warfare. Thesis finds that large number of cyberattacks are mere acts of cyber espionage, sabotage or subversion – acts which traditionally do not result in hostile actions. Additionally, due to the fact that importance of small states and involvement of non-state actors in cyberspace is increasing, diffusion of power takes place in international security environment, which challenges the stability of strategic international interaction. Two case studies are provided to strengthen the argument of changing warfare tactics, as well as to fortify importance of non-state actors on cyber escalations. This thesis argues that cyberspace is not the 5th domain of the war, however, introduction of information technologies influenced the way states conduct warfare.

KEYWORDS: cyberwar, cyberwarfare, cyber governance, cyberattack, 5th domain.

INTRODUCTION

Assumptions over changing nature of history of warfare has been arising with the advent of ethnonational conflicts, spread of democracy, end of the Cold War and nuclear revolution. The definition of warfare has been broadened by incorporating more activities and methods for competition between foes; It is notwithstanding to mention that every war incorporates warfare, whereas not all warfare tool is part of war. Introduction of Information Technologies into global scale caused similar turmoil over changing nature of war. With states exchanging cyber offences and non-state actors becoming more and more involved in cyberattacks, importance of cyber threat took higher stance on security doctrine. Immense debate over probability of the cyberwar took place between commentators since Arquilla and Ronfeldt (1993) published their article "Cyberwar is Coming!". After land, sea, air and space, number of scholars started proposing to consider cyberspace as another domain where war is being fought. Revisionists (Glenny, Kavanagh 2012; Healey 2013; Stone 2013) argue, that cyberspace has indeed become the 5th domain of the war and permission for military intervention should be expanded to offenses conducted on cyberspace. On the other hand, number of scholars (Rid 2012; Libicki 2014) take traditionalist view on war, and state that cyberspace does not answer all criteria of the classical definitions of war, therefore it is not a new war domain; nevertheless, they agree that increased cyber capabilities are changing existing state warfare tactics.

By examining the notion of war and investigating already conducted cyberattacks, this graduation thesis tests the hypothesis of cyberspace being the 5th war domain. As Harvard professor Jonathan Zittrain stated during the debate conducted by Intelligence Squared (The Cyber War… 2010):" It may not be a bomb coming down our middle chimney of our house, but it could be something that greatly affects our way of life." Undoubtedly, cyberspace poses new threats as well as new capabilities for nation-states. Research objective of the thesis is to investigate how cyberspace influences the practice of warfare. Moreover, when it comes to cyberspace and cyber power, the importance of non-state actors is evidently increasing; Thus, historiography of cyberattacks are further reviewed, in order to determine the role of non-state actors and the scale of their involvement in escalations on cyberspace.

The first chapter of the thesis sets the definitions of cyber terminology. There are no commonly agreed definitions of cyber terms. Therefore, it is essential to clarify what is considered behind terminology in this paper. Furthermore, for the purpose of examining if cyber offences conform with the war actions, secondary sources, such as classical military thinkers' works, and contemporary analysts' articles are used for literature review. Moreover, chapter provides theoretical framework and International Relations theorists' viewpoints on cyber offences, for the purpose of determining how IR theories explain developments on cyberspace. Due to the lack of literature of theoretical studies on cyberwarfare, as well as nearly non-existence of international norms and agreements, cyberspace has formed itself as non-permissive environment. Chapter analyzes how the three existing IR theories: Realism, Liberalism and Constructivism explain the nature of cyberspace and what is their suggested framework for peaceful international interaction over cyber issues.

Previous study (Rid 2012) has shown that most commonly used cyberattacks are acts of espionage, sabotage or subversion. The following chapter formulates the essence of these acts and examines how invention of cyberspace has reshaped them into politically motivated instrumental cyberattacks. Indeed, states have started utilizing cyberspace for espionage, sabotage or subversion more and more frequently. Cyberspace having low barriers of entry made cyber tools attainable for anyone with sufficient knowledge and capabilities. The chapter demonstrates how cyberspace influenced covert actions between foes. By becoming "cybered", utilizing espionage, sabotage and subversion as political tools became cheaper and accessible for not only great powers, but for small states, as well as non-state actors. Great number of the cyberattacks to-this-date are representing examples of cyber espionage, sabotage or subversion - cyberattacks which traditionally do not result in political antagonism. By providing examples of state-to-state cyber offences chapter investigates whether previous cyberattacks have resulted in warlike escalations.

The last chapter of the thesis provides case studies of two most significant cyberattacks for the doctrine. The cyberattack on Estonia in 2007 has been called by Estonian president Toomas Hendrik Ilves as "Web War I' from the tribune of UN General Assembly in 2012. While cyberattacks on Georgia in 2008 is the first instance of cyber offences accompanying ground combat. Due to the cyberspace being arena where attacker can successfully cloak its identity, evidence of who stood behind attacks on two post-soviet countries stays unattainable.

Nevertheless, allegations were made that in both instances Kremlin has utilized its cyber militia to successfully achieve its political intentions. Case studies are provided to investigate the importance of including non-state actors into international cooperation and governance over cyberspace; furthermore, by exploring how adversaries used cyber offences to foster desirable political outcome, case studies contribute in determining if with the presence of cyberspace there is an ongoing change in warfare tactics. Indeed, not only advantages followed invention of the Internet, but states and entities were introduced with new vulnerabilities, as well as new opportunities for conducting warfare.

For examination, understanding and description of existing cyber phenomenon, paper utilizes qualitative research methods. The thesis uses discourse analysis as the method for analyzing classical definitions of war and understanding the essence of political instruments. Holistic perspective, which emphasizes on the importance of the research materials as the whole, are utilized for archive research and studying historiography of conducted cyberattacks, as well as for determining how IR theories explain developments on cyberspace. Case studies of cyberattacks on Georgia and Estonia are further provided to deepen the probability of thesis findings.

1. THE CONCEPTUAL FRAMEWORK OF CYBERWAR

1.1. Defining Terminology

Clear definition of terms is essential, for the purpose of understanding the terminology used in this paper, to describe various actions or phenomenon. Different scholars define cyber terminology with different regards, due to the novelty of the subject. Cyberwar is considered as hyped phenomenon among some scholars, as others generate an idea of cyberwar being totally destructive. Therefore, understanding of basic cyber concepts is necessary to form an opinion about the probability of destructive cyberwar.

Cyberspace.

US Deputy Secretary of Defense William Lynn (2010, 101) emphasized that cyberspace being man-made domain has increased its importance on as high level as land, sea, air and space are for military operations during the war. Cyberspace being man-made domain is agreeable among scholars but providing clearly structured definition of it is problematic. Different states define cyberspace differently, nevertheless they all agree that cyberspace is a "global domain within the information environment" (Cyberspace Operations 2013, V).

There is one common definition of cyberspace, which defines it as the space incorporating all computer systems, networks and even those computers which are not connected with the internet, this kind of computers are referred to as air-gapped systems. Some scientists do not include air-gapped systems as being part of cyberspace, but this paper uses definition of cyberspace with air-gapped systems being part of it.

Sometimes those three elements of cyberspace can be overlapping with each other; therefore, to define cyberspace more distinctly Lukas Kello has determined cyberspace being the sum of overlapping terrains, such as: the internet, the world wide web and "a cyber "archipelago" comprising all other computer systems that exist in theoretical seclusion." (Kello 2013, 17).

What comprises Internet is a huge number of networked computers. But air-gapped computers and their operational systems should also be counted as the part of the cyberspace; generally, state's critical infrastructures are operating on them, as air-gapped systems are considered more secure from cyberattacks.

Cyberattack

Cyberspace is indeed one of the best inventions of humankind, but there has been fears evolving over turning it into dangerous battlefield. With the increase of its popularity, new type of threat has developed – the threat of cyberattack. Anyone who has operational computer system and sufficient knowledge can conduct a cyberattack.

Cyberattack uses code to inhibit the functionality of a computer system for the political or strategic purpose (Kello 2013, 19). The goal of an attack does not necessarily need to be constrained inside the cyberspace. An attacker may have intention of disrupting the computer system, or affecting country's functioning economic or political institutions, or degrading its social functions. Therefore, cyberattacks have direct and indirect effects. Former being to affect targeted machine, while latter refers to the consequences outside cyberspace.

This paper defines a cyberattack as targeting vulnerabilities of a nation-state from another nation-state, or non-state actors driven by national affiliation and encouraged by state government, for the primary purpose of achieving political, social or economic objectives in or through cyberspace, by interfering with the functionality of the computer systems.

Cyber power

International politics is about the influence and power struggle between political actors. Generally, power means the capacity of having an ability to receive favorable outcome by influencing people and their decisions. Therefore, cyber power as Valeriano and Maness (2015, 28) define it, is having an ability to control and dominate cyberspace. With the barriers of entry being low, scholars became cautious of non-state actors becoming able to leverage cyber power. If states are able to dominate offenses on sea or land, fears started arising that diffusion of power between state and non-state actors might happen in case of cyberspace. Nevertheless, as Nye (2010, 1) puts it - diffusion of power on cyberspace does not mean replacing power of governments with the power of non-state actors. Monopoly of power in cyberspace still stays in the hands of government. Nevertheless, due to the secrecy in cyber domain, measuring state's cyber power is challenging, therefore determining whether there is balance of cyber power between international actors or not is near-impossible.

Cyberwar and cyberwarfare

When it comes to cyberwar and cyberwarfare it is essential to clearly distinguish them from each other. Cyberwarfare concerns the conduct of war, like the warfare itself, it is executed in order to advance the combat in physical domain of the war. While the concept cyberwar means direct effect on the will of the opponent.

Some scholars agree that the concept of cyberwarfare is poorly bounded (Ormrod, Turnbull 2016, 282), there is no clear framework to define whether cyberattack is an act of war or if it is part of the cyberwarfare. For this reason, paper takes the definition of cyberwarfare, provided by Ormrod and Turnbull, as the cyberattack between two states with an intention of degrading (Ibid):"

1. *National will or ability to perform combat operations;*
2. *Government and community's ability to perform critical civic functions; or*
3. *Competitive advantage of national industry in the global marketplace."*

Paper uses Nye's interpretation for defining cyberwar as a: "hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence." (Nye 2011, 21).

Definitions are provided for the purpose of differentiating between terminologies and between cyberwar and cyberwarfare. Paper asserts that past examples of states utilizing cyberattacks, have shown that standalone not one conducted cyberattack represent an act of war, but they are mere examples of cyberwarfare, which mainly contribute in facilitating military operations or helping states to achieve its politically motivated instrumental objectives on lower cost and higher proficiency.

1.2. The Concept of War

The main contributor to the formation of the borders of the nation-states, which we face today, have been series of armed conflicts between different types of units, for the purpose of dominating each other. Essentially, war is the central concept for the study of International

Relations. There have been different thoughts over defining the characteristics of the war, nevertheless Clausewitz's version is generally agreed to be concise. The most broadly used quote from Clausewitz's "On War" is written on the very first page of the book: "War is thus an act of force to compel the enemy to do our will." (Clausewitz 1993,83). The violent character is indisputably present and vital for the conduct of war. If the lethality is not present, it is problematic to describe the conflict as an act of war. As Correlates of War Project estimates (Singer and Small 1972, 419), 1000 battle-related fatalities are essential to distinguish less level of violence from an act of war. Number of international relations theorists perceive war as "large-scale organized violence between political units" (Bull 2002, 178; Levy 1983, 215; Vasquez 1993, 378).

Clausewitz further explains why violence is necessary. If the violence has no political context, using it is illogical, stated military thinker:" The purpose is a political intention, the means is war; never can the means be understood without the purpose" (Clausewitz 1993, 90). Those maxims of war have been the contributors for conceptualization of the war during the cold war: - countries have been using violence for achieving their political goals. The way war is conducted may have changed in post-cold war era and especially with the presentation of cyberspace, nevertheless use of violence is vital for an act to be perceived as an act of war.

Another profound military strategist Sun Tzu lays out plan of action in his book Art of War for military leaders. He considers necessity of elimination of surprise military attack as one of the main goals of the leader (Sawyer 1994). As for the justified offensive operations, Sun Tzu only counts them inevitable in case of response to a direct threat (Ibid). After analyzing the essence of cyberattacks, one can conclude that cyberspace is an offense-superior domain, where basic strategies for defense or attacking an opponent have not still been determined. Therefore, Sun Tzu's definition concerning characteristics of war does not happen in cyberspace.

Not only Clausewitz and Sun Tzu agree on violent character of war, but many profound political scientists have described war as organized violence which is designated for achieving political ends. As Barkawi and Brighton (2011, 136) highlighted it, violence is "the basic element of the ontology of war." Moreover, Max Weber formulated an idea of modern state having an authority and monopoly in the given territory to exercise its legitimate military power. Therefore, nation-states have legitimate right for using physical force inside their territorial sovereignty. Quincy Wright (1964, 7) has improved even further state's right for use of violence, by explaining war as:” the legal condition which equally permits two or more hostile groups to carry on a conflict by armed force.”

History does not yet recall any cyberattack where consequences have been violent. The use of cyberweapons does not seem to have an outcome likely to the conventional sequel of interstate war. Nevertheless, cyberweapons can contribute in causing consequential harm to national or international security, but the damage of cyberattack is far from the destruction done by conventional weapons of war. Therefore, counting cyberweapon as the weapon of war might be misleading, as well as ascribing cyberspace to the domain of war. Nevertheless, on the examples of cyberattacks one can notice how utilizing cyber offensives to achieve political outcome or utilizing them during the war, have changed the nature of warfare. States tend to favor soft power over hard power with the advent of increased cyber capabilities.

The Internet worm Stuxnet is known to be invented to aim nuclear facility in Iran. Scholars argue that more than one government stands behind its creation (Schneier 2010). Creation of Stuxnet as well as its realization took multiple years. Towards the end of Bush administration, Israel became furious over Iran’s advent on enriching uranium. “Believe him and stop him” was the line used by Netanyahu concerning advancement of Iranian nuclear program (Hirschberg 2006). Israeli officials have internationally asserted about Iran’s race to atomic bomb and demanded actions to be taken to stop country from acquiring the most destructive weapon known to the world to date. Former CIA and NSA director – General Michael Hayden and counterterrorism expert Richard A. Clarke gave an interview for Zero Days documentary on Stuxnet in 2016 and stated that - Israel had intention to militarily intervene and stop Iran from obtaining nuclear bomb in 2006. Military attack never happened, however Stuxnet did. Due to the high level of secrecy over Stuxnet, it is uncertain how many nations stood behind it. However, it is obvious that with the help of cyber capabilities use of hard power and violent actions have been replaced by non-violent cyberattack. In case of Stuxnet cyber sabotage had replaced conventional military action. More on that will be discussed in next chapter of the paper.

Doctrines of Jus ad Bellum and Jus in Bello incorporate set of rules to conduct war under international law. Jus ad Bellum concerns legitimate reason for the war to be permitted. It highlights the necessity of just cause and just goals of the war, be it the reaction of the state to defend its sovereignty or other. Under Jus ad Bellum official decision and public declaration of war has to be present. In case of cyberattack, or cyberwar, respecting the international law and the doctrine of Jus ad Bellum is near-impossible, for the reason of cyberspace being the field where attackers can operate covertly and cloak their identities. After an attack on state's cyberspace, reacting on it by declaring war on offender is problematic, as attribution of an attack in cyberspace is not fast enough for timely retaliation, as well as cyberattacks up to date have not caused sufficient level of destruction. Attribution difficulties are the most vocal problem concerning cyberattack. Identity of the adversary is perfectly concealed under the enormous degree of anonymity provided within cyberspace.

Another problem which occurs is malware crossing different sovereign states before conducting an assault (Kello 2013, 33), therefore while following the cyberweapon to determine its primary source, state actors are most likely to require cooperation from multiple jurisdictions, which additionally necessitates nonexistent international cooperation on cyberspace. For the upper stated reasons, after being attacked in cyberspace, it requires ample guesswork and sufficient amount of time for the state's national security institutions, at least for determining who their enemy is. One of the most fundamental principle of the war is an idea of "enemy" (Teixeira 2009, 98). Undoubtedly, when the sovereignty of the state is attacked, it is essential to materialize the opponent in order to know who country is fighting with. While soldiers in uniform display their identity, attackers in cyberspace conceal it. Therefore, promoting domestically the declaration of war, on the offender of cyberspace is difficult to achieve. Another obstacle to domestically promote retaliation after attack on cyberspace is that cyberattack lacks capacity for violence. One can assume, that harm generated after cyberattack is unlikely to have the sufficient dose of destruction to justify going into war to the population of attacked country. It is difficult to imagine such thing as the violent cyberwar; or cyberattack generating consequences which will result in violence and casualties. However, cyberattacks do facilitate achieving military objectives on lower costs.

Assumptions over changing ways of conducting warfare have been generating since the end of the Cold War, nuclear revolution, ethnic and national conflicts and the emergence of democratic states. There are two contradictory thoughts concerning the changing nature of war. Debate between traditionalists and revisionists concerns the definition of war. Expansionists argue that neither classical definition of war, nor how law of armed conflict defines it, is adequate; they emphasize that the notion of war should expand and incorporate variety of acts, which traditionally would not be considered as an act of war. While, traditionalists argue that current definition of war is completely sufficient and does not require to incorporate new domain in it; they agree that the way warfare is conducted may change, fundamental characteristic of war which incorporates violence, damage and use of force for political purposes by state actors, stays the same. Debate over cyberwar has taken the shape of debate between expansionists and traditionalists. Thinkers like Carr (2011) argues that cyberspace has to be declared as the 5th domain of the war; While Thomas Rid (2011) argues that cyberattacks are politically motivated actions in cyberspace, which does not have sufficient characteristics to become a new domain of war. The conducted cyberattacks are not portraying new innovative elements of warfare, but taking old exercised instruments of warfare to cyberspace, or facilitating military operations, therefore ascribing cyberspace to war domains tends to be misleading.

1.3. International Relations Theories and Cyberwar

If an idea of cyberwar and cyberspace becoming a new domain of war has caused controversy among scholars, they all agree on the importance of cyber security on the agenda of international relations. Introduction of digital advancement has indeed changed the way states interact and the way they conduct warfare. Unfortunately, there is scarce literature on how international relations theories interpret IR on cyberspace. This sub-chapter will attempt to determine what are the thoughts of IR theories concerning the “State of Nations” in emerging arena of cyberspace, which has international importance. Furthermore, sub- chapter will focus on how Informational Technology is incorporated with traditional mechanisms, which cause war and peace.

Realists perceive international relations as inherently conflictual, where these conflicts are necessarily resoled by the means of war. National security and the survival of the sovereignty is the main purpose of the state (Jackson, Sørensen 2013, 66). An idea of international arena being the space where states defend their national objectives and the security of the state interests by the means of conflict and war, or in other words “power politics”, is shared with other classical theorist of Realism: Thucydides, Machiavelli, Hobbes. Thus, the idea of International Relations being anarchic finds its way as the main principle in realist theory. In this anarchic international state system, the only political actors are states, without having higher authority. And they have to defend their interests with any means. In realist view, even in this anarchic IR, there is a hierarchy of states comprising by dominant powers and weaker states which are less important, as the power struggle takes place within great powers. Therefore, from realist point of view, states will attempt to dominate cyberspace by acquiring powerful cyberweapons to achieve supremacy over its rivalries.

Lucas Kello (2017a, 212-214) defines that "cyber arms race" between great powers is already taking place on cyberspace, as states become aware of increasing militarization of this area. Furthermore, militarization of cyberspace can be a result of uncertainty in this domain. Given anarchy in cyberspace matches with Mearsheimer's (2001, 30 – 32) five postulations of offensive realism: 1. There is no central authority in this anarchic system; 2. Dominant powers hold offensive military capabilities; 3. Actors in international system can never be definite about other actors' intentions; 4. Primary goal is survival; 5. Dominant powers are rational and think through survival strategy. Arquilla and Ronfeldt (1993) declared about the cyberwar being on its way, realists would be in the same opinion with scholars, as today's cyberspace is nothing but anarchic.

As Schelling puts it: "The threat of war has always been somewhere underneath international diplomacy." (Schelling 1996, 170) Strategic realist thinker also describes international cooperation as "diplomacy of violence" (Ibid). But with the concept of balance of power (Waltz 1979, 204), which conceives bipolar system in international dominance of authority, more stable environment is provided. However, when it comes to cyberspace, due to the secrecy around cyber capabilities of great powers, one cannot determine whether balance of cyber powers is present in international order or not. Additionally, there is high probability of multipolarity in cyber power; if during cold war there have been two great powers, who had wide nuclear capabilities and as realists perceive this bipolarity became guarantee for peace, in cyberspace small nation-states, like North Korea or Israel, tend to have equal or maybe greater cyber capabilities then US or Russia. Moreover, for realists only actors in international relations are nation-states, nevertheless in case of cyberspace non-state actors are becoming more and more engaged in conducting cyberattacks. Consequently, realist IR theory lacks ability to explain relative peace in cyberspace, as anarchy is constantly present and therefore international actors are constantly in Hobbesian "state of Nations" or in "Bellum omnium contra omnes", but no big scale cyber offensive has yet happened.

Constructivists fear that the threat of cyberwar might become self-fulfilling prophecy. Wendt (1995, 73 - 75) emphasizes that international relations depend on the communication between states, which facilitates creation of state's interests in foreign affairs, therefore unlike neorealists, constructivists claim that state identities and objectives are not inherited, they are created during the interaction with other states. With fears about destructive outcome that would follow war on cyberspace and exaggerated threat, which are circulating in society, IR theorists are cautious that militarization of cyberspace might be unavoidable, in otherwise free societies.

On the contrary of realism's pessimistic view on international relations, Liberalism adopts optimistic one. John Locke being one of the contributors in developing liberalism in IR, believed in the positiveness of human nature and human reason. Liberals identify international relations as the realm, where rationality can be adopted. Collaboration and cooperation nationally and internationally are achieved on the grounds of actors having mutual interests. All this is possible as the lust for power is overshadowed by the human reason. Like other liberal thinkers, Kant also perceived international state of nature as unjust and saw the urge of departure from it by the means of international agreements and covenants. Physical realm of international cooperation accounts tremendous number of agreements and legally binding international laws, while virtual realm of cyberspace have scarce, nearly inexistent number of it. Concerning cyber security dilemmas, structural liberalist thinkers (Deudney, Ikenberry 1999) suggest that cooperation and consensus building in cyberspace is fundamental, but how to achieve them is under question. Moreover, there is a tendency of lack of agreement and cooperation concerning cyberspace in IR. International relations for liberal tradition is described as cooperation instead of conflict. Therefore, as Joseph Nye suggested, liberals are lobbing for international agreements over cyberspace to avoid conflicts.

Nye further explains that forming cyber security strategy in international relations by the means of cooperation among states is essential but problematic, due to the nascent characteristics of cyberspace. Kello (2013) repeatedly emphasizes about the lack of capacity of current international relations theories to contribute to the study of conflicts in cyberspace. He further states that cyber threat would cause unparalleled harm to international interaction (ibid, 8). If Kello contemplates over changing ways of interaction between international actors, others (Lindsay 2013; Gartzke 2013) argue that states would not fully utilize their cyber capabilities, due to the presence of sufficient constraints on them. There is an interesting pattern of states engaging in deeper cooperation between each other after being attacked on cyberspace. For example, Iran's nuclear deal was established after Stuxnet attack and consequent Iranian cyberattacks on US; or China and United States, who seem to cooperate more after cyberattacks, this could be due to the insufficient damage which do not result in political antagonism.

In his article, Gartzke (2013) underlines the distinction between what is possible and what is probable in cyberspace. He argues, that states would not engage in massive cyber offenses against each other, because their rationality would dictate so, in order to avoid consequences of it. Furthermore, the high probability of cyberspace being multipolar in terms of power is agreed upon. As Keohane (1993, 271) explains, multipolar anarchic IR system lacks trust between states, destabilization caused from it can be eliminated by institutionalization in international affairs. Jeremy Bentham further emphasized that states respect international law in foreign affairs as it is inherited in their rational interests (Rosenblum 1978, 101).

However, Lucas Kello (2017b) suggests that none of the IR theories are ready for setting theoretical guideline when it comes to interaction on cyberspace. If liberal IR theory suggests cooperation, Kello (Ibid, 228) takes it further and suggests global governance approach for cyberspace. He also perceives that with global governance, "power diffusion" would be eliminated, as the approach would also incorporate interaction and control over non-state actors (Ibid, 207). If realists do not perceive non-state actors being part of IR, liberals are more prone to it, that is yet another reason to account liberal IR theory more suitable to form theoretical framework for international interaction over cyberspace.

Overall, after investigating whether characteristics of cyberattacks and characteristics of war actions coincide, chapter concludes that cyberattacks do not conform with warlike escalations, though they do affect the conduct of warfare. To strengthen this argument, next chapter outlines examples of past state-to-state cyberattacks, which are grouped as cyber espionage, sabotage or subversion, as previous studies showed that these three types are the most commonly used cyberattacks.

2. CYBERATTACK AS ESPIONAGE, SABOTAGE AND SUBVERSION

The nature of cyberattack on state's cyberspace can vary, depending on the means it is carried out and depending on the purpose of cyberattack. This chapter focuses on three most commonly known and used forms of cyber activities: cyber espionage, sabotage and subversion. These three acts have been accompanying military operations in past, with the invention of cyberspace they became "cybered". Activities are discussed and analyzed. Firstly, Sub-chapters provide definition of the phenomenon, its essence and necessary means to utilize them, as well as examples of infiltration of state's cyberspace are provided, which had primary focus on exploiting attacks on adversary's cyberspace for the purpose of espionage, sabotage or subversion.

2.1. Cyber Espionage

Offensive activity such as espionage has been exercised between nation-states for many decades now. If before rivalries mostly used spies for the purpose of gaining secret information, today using cyberspace for clandestine operations is more sufficient. Espionage incorporates penetration of another state's military or industrial secrets. The purpose is only to gain information, not achieving any specific goal; therefore, espionage does not have instrumental character. With the gradual increase in utilizing cyberspace, state's espionage activities are more and more shifting from human intelligence services to signals intelligence services.

NATO Cooperative Cyber Defense Centre of Excellence has been established in Tallinn, after the cyberattack on Estonia in 2007. Under its initiative more than twenty experts have been working on drafting legally non-binding set of rules of international law concerning activities conducted in cyberspace. An academic study is commonly known as Tallinn Manual. It provides the definition of cyber espionage as: "any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party." (Tallinn Manual… 2013, 159).

Espionage is the most sponsored tool within cyber capabilities of the state (Rid 2012, 20). Due to the enlarged digitalized environment, the number of actors conducting espionage through cyberspace has increased. Therefore, competition between state sponsored hackers and private individuals, who are acquiring and selling data, has enhanced. The paper does not incorporate cyber espionage conducted by non-state actors for their own gain, it only concerns information gathering from state sponsored entities.

Tallinn Manual on the International Law Applicable to Cyber Warfare has incorporated state sponsored conduct of cyber espionage in its non-binding academic study. Rule 66 determines that, while adversaries are engaged in armed conflict, attempts of gathering information by cyber espionage or other means are not in violation with the law of armed conflict. Moreover, authors of manual do not consider cyber information gathering, which is conducted outside the sovereignty of attacked state, as an act of cyber espionage (Tallinn Manual… 2013, 159). When it comes to the nature of gathered information, the minority of the group of international experts took the stance of only incorporating cases of gathering data of military value as an act of cyber espionage; while majority agreed on neglecting the nature of information while dealing with cyber espionage (Ibid, 160).

Recently, United Kingdom's Government Communications Headquarters, which comprises intelligence, security and cyber agency, has estimated that 34 nation-states have well-developed capabilities of cyber espionage, targeting friends and foes (Ward 2018). Empirical study determines that cyber espionage is the most broadly used offences conducted between states (Rid 2012, 20).

It is widely known that North Korea incorporates around 6,000 hackers, working for the direction of gaining funds for its nuclear program by attacking banks in Poland and Bangladesh (Greenberg 2018). Apart from using cyberattacks for stealing billions of dollars, state is blamed for conducting cyber espionage. There is a consideration of ascribing an attack at Sony Pictures in 2014 to Lazarus – state funded hacker group from North Korea (Sanger, Perlroth 2014). The motive behind an attack has been attackers' demand to cancel release of the movie "The Interview". The plot of the movie is perceived to be unacceptable from North Korean perspective, as it incorporated the leader of the state in an intolerable way. During an attack, hackers were successful in wiping out big amount of data from corporate computers, it is also believed that couple of thousands of terabytes have been stolen. US officials accused North Korea for conducting attacks on Sony Pictures, nonetheless experts have not been able to confirm it and North Korea has denied having ties with an assault.

Another state sponsored hackers' group from North Korea, under the name APT37 has recently became known for the public, with released report by FireEye (Greenberg 2018). As the report suggests, the group has been focusing on cyberattacks on South Korea, therefore it remained less popular than Lazarus. Nevertheless, FireEye determined that lower profile of APT37 does not meant less resources or capabilities. On the contrary, the group reportedly has broad range of penetration techniques. FireEye has tracked various spy tools in the possession of APT37, designed to steal screenshots, passwords or dig through victim's files. The group is perceived to mostly aim its cyber espionage tools to the cyberspaces of South Korea, Japan, Vietnam and Middle East.

Undoubtedly utilizing cyberspace for political purposes is in the interests of smaller nation-states. Unlike conventional methods for spying and gathering information, cyber espionage needs less financial contribution. Countries can achieve their goals of infiltrating classified data and collecting sensitive materials on targeted state's critical infrastructure by utilizing less effort and funds by the means of cyber espionage. Incorporating cyberspace for data gathering does not seem to have less importance for the bigger states. The more advanced country is, more cyberspace capacities it has and therefore stronger tools it owns for conducting cyber espionage.

As early as 2003, United States has detected number of attacks on its military and governmental computer systems (Nakashima, Krebs 2007). As determined, an attack has been conducted for years. It is uncertain whether attackers have been operating through computers based in China, or if Chinese security agencies were involved. Reportedly, invaders of US's cyberspace have infiltrated Homeland Security's, the State Department's and Pentagon's numerous firewalled networks. Even though classified networks have not been included in the scale of attacks (Graham 2005), hackers succeeded in stealing around 20 terabytes of data from Department of Defense networks.

Another allegedly Chinese conduct of cyber espionage is known by the name of GhostNet. Team of researchers from the University of Toronto shared report in 2009 (Deibert, Rohozinsky 2009, 47). They have detected sophisticated mechanism designed for international spying operations. Numerous embassies, Ministries of Foreign Affairs, News media agencies, International organizations and NGOs have been aimed for the purpose of gathering information in 103 countries. The level of penetration of the affected computers incorporated downloading documents, obtaining recorded information and even activating cameras and microphones of computers.

Despite widened national security policies aimed at defending secret military and industrial information from being infiltrated by cyberattacks, the scale of cyber espionage is thriving. In his article "Hacking is the New Face of Espionage", Eric O'Neill (2016) calls on the new technologies being contributor in completely changing face of the way espionage is being conducted nowadays. Indeed, achieving political goals by the means of infiltrating adversaries' cyberspace is becoming more and more widespread with the advancement of technologies. However, not only cyber espionage is not an act of war, it is not considered to be crime by international law and furthermore it is less likely to become contributor in starting war between two states.

2.2. Cyber Sabotage

Another widely used offense in cyberspace is cyber sabotage. Sabotage itself is a deliberate act to destruct or damage facilities for the military or political advantage. Conducted in the cyberspace, sabotage can achieve its objectives with less costs and determining an offender is less likely. Cyber sabotage does not always result in physical damage or violence, even though its primary objectives are mainly physical targets, but not human beings. Cyber sabotage is usually used for achieving tactical objectives, even though it might result in strategic goals, although it is less likely. More country and its military and governmental systems depend on technical developments, more likely it is that adversary will use cyber sabotage against the state. Sabotage has an instrumental nature, as saboteurs tend to avoid excessive violence and political attribution, as the ultimate goal of cyber sabotage is diminishing and weakening technical systems.

There are series of cyber sabotage examples known for the public, nevertheless most of them tend to lack official attribution. Some examples of cyber sabotage have happened alongside with conventional military offences. The most widely known example of it is Israel's bombing raid in 2007 on nuclear reactor site in Syria. Operation known by the name of "Orchard" had an objective of turning one of the most capable air defense systems in the world un-operational. Israelis succeeded in blinding Syria's air defense and subsequently Israeli warplanes have entered Syrian airspace, raided Dayr ez-Zor and left again without being detected. (Fulghum, Wall, Butler 2007, 30). The government of United States publicized an attack, by sharing images of the nuclear site before and after an attack (Markoff 2010). Despite the fact that the details of an attack are classified, not much speculation is needed to conclude that without utilizing cyberattack and turning Syrian air defense dysfunctional, operation would have resulted in as much success as it did. Nevertheless, it should be noted that stand alone the cyberattack would not have constituted in physical destruction, but undoubtedly utilizing cyber sabotage facilitated the success of military attack.

When it comes to discussing cyber sabotage, one cannot avoid mentioning the most sophisticated cyberattack to date, known by the name of Stuxnet. The malware, which spread across dozens of countries and affecting numerous computer systems, had only one objective and one particular aim. Stuxnet is an example of standalone cyber sabotage, which had nothing in connection with conventional military actions. Spreading the worm is considered to be multi-year operation starting form 2007 up until 2010 (Langner 2011). It is considered that Stuxnet has been spreading through USB sticks, as it had succeeded in affecting air-gapped operational systems. The target of the malware has been determined to be centrifuges in Iranian nuclear site. An objective of Stuxnet has been changing speed and frequency of the drivers, which resulted in damaging turbines and centrifuges. Goal of the creators of Stuxnet is commonly agreed to be the delay of Iran's nuclear enrichment program. The level of sophistication of Stuxnet has raised well-based doubts on one of the "cyber superpowers" being behind it. As the German security consultant Ralph Langner stated during his TED talk speech in March 2011, creation of Stuxnet could have been unimaginable without tremendous resources and investments. As countries are inclined to abstain from publicizing conducted cyberattacks on them, it is difficult to determine whether Stuxnet has been successful in its objectives or not, but one thing is certain after Stuxnet, cyber sabotage has been established as an entirely new and successful tool for achieving political objectives.

Investigators of an incidents occurred in 2015 and 2016, which incorporated power cut on the capital of Ukraine - Kiev, have determined and act being a cyberattack (Ukraine Power Cut… 2017). Allegedly Russian sponsored attack left half of the city without electricity in cold winter nights in 2015 and 2016. President Poroshenko called cyberattack as an:" acts of terrorism and sabotage on critical infrastructure facilities." (Ibid). Annexation of Crimea by the Russian Federation since 2014, leaves little room for the thoughts on who might be behind the cyber sabotage conducted against Ukraine. Power cut on Kiev is yet another successful usage of cyberspace for the purpose of sabotage.

As NATO warplanes advanced to bomb Serbia during the war for liberation of Kosovo in 1999, several cyberattacks took place on NATO's internet infrastructure. Organization which claimed an attack called themselves "Black Hand", pro-Serbian hacker group, whose primary objective has been to disrupt NATO's military operations (Geers 2011, 81). The goal of an attack has been deleting data from NATO owned computers. While group asserted to have been successful in their attack on U.S. Navy computers, government of United States stated that it experienced "no impact" with an attack (Ibid 82). However, NATO owned website, which released briefs regarding war in Kosovo has become inoperable for several days (Verton 1999). Internet war during war in Kosovo in 1999 is yet another example of utilizing cyberspace for the purpose of sabotage.

As Thomas Rid and Peter McBurney suggest (2012, 12), brief empirical analyzes have determined military offences being more successful, while accompanied with cyber sabotage. Indeed, using cyberspace for the purpose of sabotaging adversary has wide variety of ends, be it standalone act of cyber sabotage or accompanying military attacks. It is certain that using cyberspace to weaken functionality of economic or military systems took sabotage on the whole new level. Nevertheless, it should be stated that sabotage is not considered as an act of war or contributor to war-like escalations.

2.3. Cyber Subversion

States or entities have been utilizing subversion as the tool for advancing their interests by undermining established authority, state's integrity and constitutional order of an adversary. There can be found wide variety of means of subversion in history, propaganda and other covert influence operations being the most common. The range of a goal of subverter can vary from undermining an authority of a person, to overthrowing government of a state. The ultimate goal of subversion is to damage society's trust in government by aiming and causing damage to society's beliefs and norms. Subversion does not necessarily have violent characteristics. In fact, the most commonly used form of subversion – propaganda - uses different informational technologies for achieving its goal. If in case of sabotage, the main targets of attackers are machines, in case of subversion affecting humans and their motivation is central. It should also be noted that successful act of subversion does not necessarily imply overthrow of established government, sometimes undermining an authority is the main goal of the tactic.

Subversion is considered to be limited in its instrumental character, as emotional aspects are usually aimed with the practice. Additionally, an act intends to aim at specific issue and facilitate and strengthen motivation of activists. With the advancement of information technologies and widespread access of civilians to it, utilizing cyberspace for subversive activities has become easier. Level of entry to cyber subversive activity is low, while the non-attribution benefit is present. Therefore, state can use cyber subversion on an adversary, achieve its goal with low cost and have low probability to be detected. Its attractiveness contributes in cyber subversion being used multiple times, by state actors or state sponsored hacker groups.

One of the first examples of usage of cyber subversion has been by Chechen guerilla fighters who were successful in utilizing Internet infrastructure for their expanse on the early phase of "internatization" of the world. The separatist movement is considered to be first users of World Wide Web for the purpose of spreading strong public messages during the ground conflict between pro-Chechen and Pro-Russian fighters (Thomas 2002). Chechen fighters used cyber propaganda to generate strong anti-Russian feelings in public. As leaders in Kremlin were denying an attack on Chechen civilian bus and subsequent killings of numerous passengers, guerilla fighters have spread images which were describing an incident (Goble 1999). Furthermore, Chechen separatist movement has been streaming online videos of their military activities (Thomas 2002). After utilizing cyberspace for propaganda from Chechen side, Russian officials concluded that country needed to advance its cyberspace tactics, as interim prime minister of Russian Federation, Vladimir Putin stated: "we surrendered this terrain some time ago… but now we are entering the game again." (Goble 1999). Cyber subversion from Chechen separatist movement side has been accompanying on ground military activities.

Utilizing cyberspace for propaganda has facilitated emergence of strong national feelings among Chechen nationals, additionally it strengthened financial and emotional support to guerilla fighters.

Another example of cyber subversion occurred during the rise of tensions between Chinese and U.S. government in between the bombing of Chinese embassy in Belgrade in 1999 from U.S. side and incident which occurred over the South China Sea in 2001, resulting in clash of U.S. and Chinese jets. Consequently, hacker groups from United States and People's Republic of China created portals under the name "USA Kill" and "China Killer" (Geers 2011, 84). Adversaries have been using cyberattacks for defacing numerous webpages and subsequently attempting to damage the trust of the citizens of opponent state. Both countries claimed responsibilities for the occurred cyberattacks.

As in cases of cyber espionage and cyber sabotage, cyber subversion is widely exercised by states. None of the upper stated examples of cyberattacks have caused sufficient amount of damage to result in military escalations, therefore examples of utilizing cyberwarfare tools do not result in military retaliation. Another widely publicized examples of cyberattacks have been conducted against Estonia in 2007 and Georgia in 2008. Allegedly Russian sponsored group of hackers and individuals have conducted Distributed Denial-of-Services attacks against governmental webpages, financial institutions and news media portals. During both attack with the help of Kremlin, Russian citizens driven by patriotic favors, have been blamed to be involved by accessing instructions on Russian forums for conducting DDoS attacks on Estonian and Georgian Webpages. Next Chapter will discuss cyberattacks conducted against two post-Soviet countries in more detail and try to determine the nature and purpose of attacks and how they influenced the conduct of warfare.

3. CASE STUDIES

Chapter gives an overview of cyberattacks conducted against Estonia in 2007 and Georgia in 2008. Attack against Estonia has been called as the "Web War I" by Estonian president Hendrik Ilves in his speech at United Nations General Assembly in September 2012. While Georgian case is known as the first case, when military actions have been accompanied by attacks at country's cyberspace. Allegations about who stood behind attacks were circulating in media; despite the fact that actual, lawful attribution of an attack to state entity has not been yet identified.

3.1. Cyberattack on Estonia in 2007

Tensions between Estonian and Russian states have been present before and after small Baltic state left Soviet Union. Estonian government's decision to relocate Bronze Soldier dressed in World War II Red Army uniform, in April 2007, resulted in protests from country's large Russian-speaking minority. The outrage further escalated as Russian news media reports spread false accusations, claiming that the statue – "Monument to the Liberators of Tallinn", and nearby graves of Soviet war soldiers were being destroyed (McGuinness 2017). Protests resulted in thousands of arrests, more than 150 injuries and one death. Attack on Estonian cyberspace has been followed to the violent riots in the capital. Nation of barely 1.4 million people had 760,000 Internet users when cyberattack took place in 2007 (Internet World Stats 2014a). By 2007 country has already been known as having one of the most advanced e-government systems in Europe. Attackers used Distributed Denial of Services attack, which lasted over three weeks, and which left highly internet integrated country vulnerable.

Cyberattacks aimed at multiple critical infrastructure for social, political and economic spheres of the state: Estonian Presidential webpages, Parliament webpage, ministerial webpages including ministries of Justice and Foreign Affairs, two of the biggest banks operating in Estonia (one of them being of Swedish origin), three biggest news media organizations, political parties and firms specializing in communications (Traynor 2007). The element of cyber propaganda has been present during an attack, webpage of Estonian Prime Minister's political party has been defaced and the message of apology and promise to move the statue to its primary location has been spread (Geers 2011, 85).

Estonian authorities reacted by closing down attacked webpages to the access from foreign internet addresses, which left sites under attack accessible for domestic users. Cyberattacks on Estonia have become the first precedent of cyberattacks on an entire country. Estonian Cyber Emergency Response Teams succeeded in building firewalls and utilizing additional human and technological resources for achieving filtering out malicious data by the end of the first week of attacks (Landler, Markoff 2007). However, determining who stood behind DDoS attacks which requires at least sufficient amount of human resource, became problematic. Determining initial source of attacks further exacerbated as Moscow refused to aid Estonian investigators. Nevertheless, CERT determined that cyberspace of 100 national jurisdiction has been crossed in the process of cyberattacks, as stated most IP addresses have been of Russian origin.

Estonia being member of NATO considered invoking article V, which incorporates: “an armed attack against one [Alliance member] … shall be considered an attack against them all” (The North Atlantic Treaty 1949). However, apart from being unable to attribute attack to any state, Estonia was unable to provide evidence that cyberattack had the scale of an armed attack. Moreover, despite the fact that most of the initial sources of attacks have been hackers from Russia, and some of IP addresses of initial attacks determined to be from Russian state institutions, finding concrete evidence of Russian government's involvement to carried out attack was challenging. As one of the Estonian Government Official stated to BBC, it has been determined that initial cyberattacks were orchestrated by Kremlin, while gangs of hackers seized the opportunity to contribute in the aftermath (McGuinness 2017).

An attack at Estonian cyberspace has contributed in moving cyber security on the higher level of visibility in the dialogue for international security for NATO's strategic concept. Furthermore, NATO Cooperative Cyber Defense Centre of Excellence has been established in Tallinn in 2008. A group of international experts have been working on drafting Tallinn Manual - legally non-binding set of rules concerning attacks conducted in cyberspace. Rule 20, article 3 of Tallinn Manual determines that:” the law of armed conflict did not apply to those cyber operations [against Estonia] because the situation did not rise to the level of an armed conflict." Furthermore, Rule 7 of the Manual states that even if cyber operations are originated from governmental cyber infrastructure, it does not necessarily mean that an attack should be attributed to the state; nevertheless, state might be associated with an attack. Number of experts (Gervais 2012, 540; Nguyen 2013, 1123 - 1124), agree that cyberattacks on Estonia did not constituted in the scale of an armed conflict. However, the sovereignty and non-intervention principle has been largely breached.

Despite the fact that security specialist determined attacks being conducted by group of people, with minimal interference of governmental infrastructure, denial of Moscow to cooperate with Estonian investigators leaves question marks. Be it conducted by state or non-state actors, an attack had clear objectives of cyber subversion. Having discontent of Russian speaking minority on the plate, authority of Estonian government has been further damaged by cyberattacks on state's economic, social and political institutions. An attack set an example of how hostile nation-states can utilize cyber subversion during probable tensions on an adversary state. As well as set an agenda for international community to establish strong communication and cooperation on the issues concerning cyber security. Moreover, cyberattack on Estonia emphasized the need of incorporating non-state actors to security discussions.

3.2. Cyberattack on Georgia in 2008

Long territorial dispute and provocations from Russian side, resulted in armed confrontations between Russia and Georgia in August 2008. The war officially commenced on 7th of August 2008, with Georgian military forces expanding towards the town Tskhinvali located in Russian occupied territory of South Ossetia. As the response Kremlin deployed additional forces to South Ossetia, which resulted in defeating Georgian military forces and consequential advance of Russian military and Ossetian militia into Georgian controlled territory. Military operations against Georgia halted as ceasefire agreement has been signed a week later. As the result, Georgia further lost territories to the Russian occupation.

With bombs shelling down on the Georgian soil, massive cyber offensive against country's cyberspace has started. Nevertheless, security specialists have determined that before massive cyberattacks during war in August, Russian-supported hacker militia has attacked Georgian cyberspace as early as July 2008. Numerous Georgian servers, Presidential webpage being amongst them, have been flooded with the following message:" win+love+in+Russia" (Thomas 2009, 56). Number of experts determined July attack to be the "dress rehearsal" before August (Ibid).

In case of Georgia, cyberattacks have been accompanied with ground combat. Like in Estonian case, allegedly Russian patriotic hackers have used DDoS attacks, which results in a denial of services and prevents the use of computer services. Attacks have been conducted in three stages. During the first phase, governmental websites have been defaced, when users tried to open them in their browsers, they saw pictures of Adolf Hitler and interim President side by side. Picture sent a message to the Georgia citizens of how Saakashvili's governance resembled to the regime in Nazi Germany. Second phase of cyberattacks resulted in shutting down national bank's webpage, public and private sector's webpages, news media networks and governmental webpages. The third phase incorporated spreading malicious software, as Russian coder Stroikov stated in *Хакер* ("Hacker") magazine (Shachtman 2008), SQL injection has been used to infiltrate Georgian Parliament webpage.

During the attacks on Georgian cyberspace, country has been receiving Internet through landlines coming from Turkey, Armenia, Azerbaijan and Russia. Nevertheless, there is no evidence of attempting to disrupt this connection in physical or virtual level (Zmijewski 2008). The absence of physical damage to Georgia's Internet infrastructure formulates an idea among some scholars that an objective of the cyberattacks against Georgia has been to "isolate and silent" country during the ground war (Shakarian 2011, 66). Furthermore, defacement of webpages has been considered as the acts for propaganda purposes, trying to generate negative attitude in Georgian society towards interim president.

Despite the fact that Georgia has been in ground war with Russia, attribution of cyberattacks has become problematic, as Kremlin denied having any ties with attacks on Georgian cyberspace. Various websites have been created in Russian cyberspace for the purpose of recruiting "patriotic" Russian computer users (Danchev 2008). "StopGeorgia.Ru" which started operating in 9th of August 2008, provided simple instructions of how to conduct an attack. Be it patriotic hackers, Russian cyber militia or simply civilians acting on their own will, the fact that cyberattacks have been closely coordinated with ground combat leaves little room for doubt. As the interim chief of Georgian National Security Council stated:” Moscow cyber attacked us – we just can’t prove it” (Shachtman 2009). Rule 11 of Tallinn Manual - legally non-binding set of international rules concerning cyberattacks, states that operations on cyberspace only constitute in use of force, when its effects can be equivalent to the level of damage caused by the use of force by non-cyber operations in physical world. Despite the fact that, there has been ground combat present in Russo-Georgian war in 2008, cyber operations against Georgian cyberspace had insufficient scale of damage to be comparable to the use of force in physical world.

Cyberattacks left small eastern European state’s government unable to communicate internationally during the war, preventing telling their side of the story to international partners. Additionally, Georgian citizens were unable to access information about developments during the war, as number of news media webpages were left un-operational. Undoubtedly, primary objectives of attacks have been damaging authority of elected government, as well as leaving media unable to share news about ongoing war nationally or internationally. Isolation of the country from international community during the war, or as Kenneth Corbin put it “isolate and silence” has been achieved as the war commenced. But with the help of Estonian CERT, Georgian government succeeded in receiving access to Google blog for getting its voice heard internationally.

Lucas Kello (2013) in his article “The Meaning of the Cyber Revolution”, underlines two tactical benefits for Russian side, which resulted from cyberattacks on Georgia during Russo – Georgian war in 2008: Firstly, Tbilisi became unable to communicate and coordinate actions with its civil defense agencies; Secondly, paralyzing national bank’s operations resulted in hindering Georgia’s ability to purchase war materials from private industry. As Kello points out, achieving both objectives could have been possible with conventional war tactics. Nevertheless, utilizing cyberweapons made achieving political objectives less violent.

As during cyberattacks, Georgia has been less internet dependent comparing to its current stance, it is widely agreed that attacks had little effect on civilians. Nevertheless, tactics used has clear indications for undermining authority of government, by spreading pictures of interim president compared to Hitler, or leaving high officials vulnerable by cutting communication channels with Georgian allies. Cyber subversion against Georgia has been accompanied by ground combat operations. Cyberattacks have become facilitator during land, air and sea combat operations, to achieve Russian political objectives by utilizing cyber propaganda and other subversive activities. Number of Scholars (Geers 2011, 85; Hollis 2011, 9) argue that use of cyberattacks during conventional war might become common practice in future military campaigns. Calling patriotic hacker militia for help: to facilitate the success of combat on ground, or to succeed in distracting adversary, as well as attempt to damage government's authority domestically - is cheap, less violent and easily attainable objectives for the nation-state, therefore probability is high that states will adopt it in future. Nevertheless, standalone cyberattacks doesn't have enough capacity to result in as much objectives as when they are conducted with military operations, and other way around.

Both cases of cyberattacks underlined an importance of non-state actors becoming part of international cooperation over cyber security. Undoubtedly, utilizing cyber militia as the tool to conduct cyberattack on an adversary and undermine state authority, or achieve other political objective, is becoming widely exercised practice. Cyberattacks conducted in past are merely politically motivated instrumental acts, generally conducted by non-state actors, but mainly with the inspiration of state government. Having said that, one can conclude that "cybered" political instruments are not comprising into new war domain but transforming old practices more powerful with the help of information technology. Undoubtedly, Cyber espionage, subversion and sabotage are strong political instruments in the hand of governments and non-state actors, who are becoming more and more engaged into conducting cyber offenses, which leaves us with an assumption of essentiality to incorporate non-state actors into tools for governing cyberspace.

CONCLUSION

After analysing conducted cyber offences, thesis concluded that cyberspace is not the 5th domain of the war and is improbable to become one, as cyberattacks do not conform with the existing definitions of war; however, cyber offences are influencing conduct of warfare by making politically motivated instruments "cybered". Furthermore, thesis determined the importance of non-state actors in this manmade environment and consequent realization that international relations theories are not ready to provide theoretical framework to incorporate non-state actors into international interaction over cyberspace, therefore thesis found that, for eliminating fundamental instability on international realm, new theories or new type of governance is essential while dealing with cyber issues. Cyberattacks are means for achieving wide variety of ends. Commonly, states exercise them for cyber espionage, sabotage or subversion. On the basis of examining examples of conducted cyberattacks, thesis found that cyberspace is not an independent war domain, but an environment which facilitates warfare at different levels.

While focusing on the applicability of characteristics of war to the notion of cyberwar, it was found that cyber offences do not fall in line with the classical definitions of war; Firstly, because none of the past cyberattacks have been violent or caused an injury; Secondly, the notion of war implies the use of armed force, damage caused by cyberattacks does not seem to be significant enough to cause political antagonism between states, on the contrary, there have been examples of states engaging in deeper cooperation after cyberattacking each other (Stuxnet's case for instance); Thirdly, difficulty for attribution challenges states to determine an identity of their offender, typically, as case studies showed, state governments are conducting cyberattacks through cyber militia, or patriotic hackers are acting on their own will; this arises fourth inconsistency – while traditional notion of war implies state-to-state actions, non-state actors are playing significant part in cyber escalations.

Low barriers of entry, ability to cloak identity and asymmetric vulnerability results in smaller states and entities being able to exercise hard and soft power in cyberspace. It has been determined that there is a diffusion of power between states, and between states and non-state actors in cyberspace; however, it is worth mentioning that non-state actors do not yet have enough capabilities to replace governments' hegemony on cyber power, though they do play an important role in cyber actions. It is challenging for international relations theories to provide theoretical explanations for developments in this non-permissive environment or "state of Nations" in cyberspace. Diffusion of power further impediments classical theories' ability to predict peace or war in cyberspace; however, liberal IR theory was found to be more suitable for explaining developments in cyber dominion.

It was ascertained that states tend to use cyberspace for achieving politically motivated instruments of espionage, sabotage and subversion, which facilitates success of accomplishing their goals with the benefit of being undetected, nevertheless none of them are war actions. Examples of cyber espionage, cyber sabotage and cyber subversion has been provided, none of which caused enough political antagonism to result in warlike escalations between states. Thus, cyber offences do not have the capacity to become a foundation for violent hostilities between nation-states. Having said that, hypothesis of the paper – cyberspace being 5th domain of the war - has been further invalidated, as cyberattacks do not result in military confrontations.

While examining two widely discussed cyber offences, it has been found that warfare tactics influenced by cyberspace underline significance of the role of non-state actors. Cyberattacks on Estonia in 2007 took place during the protests of country's Russian speaking minority over the removal of bronze soldier. Estonia's sovereignty has been breached by cyber subversion, as cyberattacks have been mere attempts of undermining government's authority and rendering country's economic institutions inoperable for three weeks. Despite Estonia being part of NATO article V has not been provoked as cyberattacks have not been attributed to a state and furthermore the damage has not been significant enough to cause political antagonism. In case of Georgia, cyberattacks have been accompanied with ground military actions in 2008. Country has been in war with Russia, however attribution of cyberattacks did not take place. Despite ground combat being present, cyberattacks did not constitute in damage connected with military offences, however aim of cyber offences have been determined to be undermining interim government's authority and leaving society in informational vacuum, as well as disrupt government's ability to communicate internationally during the war. Both of the case studies further strengthened an idea of standalone cyberattacks not having sufficient level of damage to invoke political antagonism, as they tend to be yet another demonstration of cyber subversion. Moreover, case studies once again emphasized importance of non-state actors in future cyber talks, as in both cases cyber offences have been conducted by cyber militia - allegedly governed from Kremlin. Case studies further demonstrated that state's warfare tactics conducted through cyberspace are mostly carried out by non-state actors and the consideration about ongoing change in warfare tactics as been strengthened.

Overall, the findings of this graduation thesis proved that standalone cyberattacks do not represent acts of war, but are realization of politically motivated instruments, aimed at influencing adversaries by utilizing cyber espionage, sabotage or subversion. Furthermore, cyberspace affects warfare tactics in a way that non-state actors are becoming more and more involved in cyber dominion. Lack of academic theoretical writings and legal framework on cyberspace provides vulnerability of security studies of the doctrine and results in scarcity of the theoretical and legal framework for cyberspace. Further research is suggested for shaping framework of new type of governance for cyberspace which will incorporating non-state actors in international cyber cooperation.

LIST OF REFERENCES:

Address by the President of Estonia, Toomas Hendrik Ilves, to the 67th Session of the United Nations General Assembly at the UN Headquarters in New York, 26 September 2012. Accessible: https://vp2006-2016.president.ee/en/official-duties/speeches/7991-address-by-h-e-toomas-hendrik-ilves-president-of-estonia-to-the-67th-session-of-the-united-nations-general-assembly-un-headquarters-new-york-september-2012/ , 26.11.2018.

Arquilla, J., Ronfeldt, D. (1993). "Cyberwar is Coming!" – *Comparative Strategy*, Vol. 12, No. 2, 141 – 165.

Barkawi, T., Brighton, Sh. (2011). Powers of War: Fighting Knowledge, and Critique. – *International Political Sociology*, Vol. 5 Issue 2, 126 - 143.

Bull, H. (2002). *The Anarchical Society: A Study of Order in World Politics*. New York: Palgrave.

Carr, J. (2011). *Clausewitz and Cyber War*. Accessible: http://jeffreycarr.blogspot.com/2011/10/clausewitz-and-cyber-war.html , 28.11.2018.

Clausewitz, C. V. (1993). *On War*. Chronology copyright 1993 by Everyman's Library. Germany: GGP Media GmbH, Pössneck.

Cyberspace Operations, The US DOD Joint Publication (JP) 3-12, 2013.

Danchev, D. (2008). *Coordinated Russia vs Georgia cyberattack in progress*. Accessible: https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/ , 10.11.2018.

Deibert, R., Rohozinsky, R. (2009). *Tracking GhostNet.* Toronto: Munk Centre for International Studies.

Deudney, D., Ikenberry, G. (1999). The nature and sources of liberal international order. – *Review of International Studies*, Vol 25, No 2, 179 – 196.

Fulghum, A.D., Wall, R. Butler, A. (2007). Cyber-Combat's First Shot. – *Aviation Week & Space Technology,* 16 November 2007, 28- 31.

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War on the Internet Back down to Earth. – *International Security,* Vol. 38m No. 2, 41 – 73.

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

Gervais, M. (2012). Cyber Attacks and the Laws of War. – *Berkeley Journal of International Law,* Vol. 30, Issue 2, Article 6, 525 – 579.

Glenny, M., Kavanagh, C. (2012). 800 Titles But no Policy – Thoughts on Cyber Warfare. – *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy,* Vol. 34, No. 6, 287 – 294.

Goble, P. (1999). *Russia: analysis from Washington: a real battle on the virtual front.* Radio Liberty, 9th October 1999.

Graham, B. (2005). *Hackers Attack Via Chinese Web Sites.* Accessible: http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html , 20.11.2018.

Greenberg, A. (2018). *The Toolset of an Elite North Korean Hacker Group on the Rise.* Accessible: https://www.wired.com/story/north-korean-hacker-group-apt37/ , 25.10.2018.

Healey, J. (2013). *A Fierce Domain: Conflict in Cyberspace, 1986 to 212.* Arlington: Cyber Conflict Studies Association.

Hirschberg, P. (2006). *Netanyahu: It's 1938 and Iran Is Germany: Ahmadinejad Is Preparing Another Holocaust.* Accessible: https://www.haaretz.com/1.4931862 , 20.11.2018.

Hollis, D. (2011). Cyberwar Case Study: Georgia 2008. – *Small Wars Foundation: Small Wars Journal.* 1 – 10.

Internet World Stats. (2014). *Internet Usage Stats and Market Report.* Accessible: https://www.internetworldstats.com/eu/ee.htm , 20.11.2018.

Jackson, R., Sørensen, G. (2013). *Introduction to international relations: Theories and Approaches.* Fifth edition. United Kingdom: Oxford University Press.

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. – *International Security,* Vol. 38, No. 2, 7 – 40.

Kello, L. (2017a). *The Virtual Weapon and International Order.* New Haven: Yale University Press.

Kello, L. (2017b). *Cyber Security: Gridlock and Innovation.* In Beyond Gridlock, Editors: Hale, T. Held, D. UK: Polity Press.

Keohane, R.O. (1993). Institutional Theory and the Realist Challenge after the Cold war. – *Neorealism and Neoliberalism: The contemporary Debate.* New York: Columbia University Press, 269 – 301.

Landler, M., Markoff, J. (2007). *Digital Fears Emerge After Data Siege in Estonia.* Accessible: https://www.nytimes.com/2007/05/29/technology/29estonia.html , 11.11.2018.

Langner, R. (2011a). *What Stuxnet is all About.* Accessible:

https://www.langner.com/2011/01/what-stuxnet-is-all-about/ , 25.11.2018.

Langner, R. (2011b). Cracking Stuxnet, a 21st Century Cyber Weapon. *TEDtalk* March 2011. Accessible:https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon , 25.11.2018.

Levy, J.S. (1983). *War in the Modern Great Power System, 1495 – 1975.* Lexington: University Press Kentucky.

Libicki, M.C. (2014). Why Cyber War Will Not and Should Not Have its Grand Strategist. – *Strategic Study Quarterly,* Vol.8 No. 1, Spring 2014, 23-39.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. – *Security Studies,* Vol. 22, No. 3, 365 – 404.

Lynn, W. J. (2010). Defending a New Domain. – *Foreign Affairs,* Vol.89 No. 5, September/October 2010, 101.

Machiavelli, N. (1984). *The Prince.* New York: Oxford University Press.

Markoff, J. (2010). *A Silent Attack, but Not a Subtle One.* Accessible: https://www.nytimes.com/2010/09/27/technology/27virus.html , 25.11.2018.

McGuinness, D. (2017). *How a cyberattack transformed Estonia.* Accessible: https://www.bbc.com/news/39655415 , 20.11.2018.

Mearsheimer, J. J. (1990). Back to the Future: Instability in Europe after the Cold War. – *International Security,* Vol 15, No1. The MIT Press, 5 – 56.

Mearsheimer, J. J. (2001). *The Tragedy of Great Power Politics.* New York: W. W. Norton & Company.

Morgenthau, H. J. (1965). *Scientific Man versus Power Politics.* Chicago, IL: Phoenix Books.

Myers, Ph. A. (1980). Subversion: The Neglected Aspect of Computer Security. (Master thesis). Naval Postgraduate School. Monterey, California, USA.

Nakashima, E., Krebs, B. (2007). *Contractor Blamed in DHS Data Breaches.* Accessible: http://www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471.html?noredirect=on , 23.11.2018.

Nguyen, R. (2013). Navigating Jus Ad Bellum in the Age of Cyber Warfare. – *California Law Review,* Vol. 101, Issue 4, Article 4, 1080 – 1129.

Nye, J. S. Jr. (2010). Cyber Power. – *Belfer Center for Science and International Affairs.* Cambridge: Harvard Kennedy School.

Nye, J. S. Jr. (2011). Nuclear Lessons for Cyber Security? – *Strategic Studies Quarterly,* Volume 05 - Issue 4, Winter 2011. 18-38.

O'Neill, E. (2016). *Hacking is the New Face of Espionage*. Accessible: https://www.carbonblack.com/2016/10/20/hacking-new-face-espionage/ , 23.11.2018.

Ormrod, D., Turnbull, B. (2016). The cyber conceptual framework for developing military doctrine. – *Defense Studies,* 16:3, 270-298.

Raitasalo, J., Sipila, J. (2004). Reconstructing War after the Cold War. – *Comparative Strategy,* Vol. 23, No. 3, 239 – 261.

Rid, Th. (2012). Cyber War Will Not Take Place. – *Journal of Strategic Studies*, Vol. 35, No. 1, February 2012, 5 – 32.

Rid, Th. (2013). *CYBERWAR WILL NOT TAKE PLACE.* New York: Oxford University Press.

Rid, Th., McBurney, P. (2012). Cyber-Weapons. – *The RUSI Journal*, Vol. 157, No. 1, February/March 2012, 6 - 13

Rosenblum, N. L. (1978). *Bentham's Theory of the Modern State.* Cambridge, MA: Harvard University Press.

Sanger, D., E. Perlroth, N. (2014). *U.S. Said to Find North Korea Ordered Cyberattack on Sony*. Accessible: https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0 , 30.10.2018.

Sawyer, R.D. (1994). *Sun Tzu: Art of War.* Oxford: Westview Press.

Schelling, T. (1996). The Diplomacy of Violence. – *International Politics*, 4th edition, New York: HarperCollins, 168 – 182.

Schneier, B. (2010). *The Story Behind the Stuxnet Virus*. Accessible: https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html#73fbfa5851e8 , 20.11.2018.

Shachtman, N. (2008). *Russian Coder: I hacked Georgia's Sited in Cyberwar.* Accessible: https://www.wired.com/2008/10/government-and/ , 19.11.2018.

Shachtman, N. (2009). *Top Georgian Official: Moscow Cyberattacked us – We Just can't Prove it.* Accessible: https://www.wired.com/2009/03/georgia-blames/ , 28.11.2018.

Shakarian, C. P. (2011). The 2008 Russian Cyber Campaign Against Georgia. – *Military Review,* November – December 2011, 63 – 68.

Singer, J.D., Small, M. (1972). *The Wages of War, 1816 – 1965: A Statistical Handbook.* New York: Wiley.

Stone, J. (2013). Cyber War Will Take Place! – *Journal of Strategic Studies,* Vol. 36, No. 1, 101 – 108.

Tallinn Manual on the International Law Applicable to Cyber Warfare, The NATO Cooperative Cyber Defense Centre of Excellence, Ed. Schmitt, M.N. New York: Cambridge University Press. 2013.

Teixeira, A. V. (2009). Global War: The Concept of Modern War Under Attack. – *Mexican Law Review,* Vol II, No.2, 89 – 106.

"The Cyber War Threat Has Been Grossly Exaggerated". (2010). Intelligence Squared U.S. Accessible: https://www.intelligencesquaredus.org/debates/cyber-war-threat-has-been-grossly-exaggerated, 21.11.2018.

The North Atlantic Treaty. (1949). Accessible: https://www.nato.int/cps/ie/natohq/official_texts_17120.htm , 29.11.2018.

Thomas, T. L. (2002). Information Warfare in the Second Chechen War: Motivation for Military Reform? – *Foreign Military Studies Office.*

Thomas, T. L. (2009). The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia. – *Journal of Slavic Military Studies*, Vol 22, No 1, 31 – 67.

Traynor, I. (2007). *Russia accused of unleashing cyberwar to disable Estonia.* Accessible: https://www.theguardian.com/world/2007/may/17/topstories3.russia , 21.11.2018.

Ukraine Power Cut "was Cyber-attack". (2017). Accessible: https://www.bbc.com/news/technology-38573074 , 22.11.2018.

Valeriano, B. Maness, R. C. (2015). *Cyber War versus Cyber Realities: Cyber Conflict in the International System.* New York: Oxford University Press.

Vasquez, J.A. (1993). *The War Puzzle.* New York: Cambridge university Press.

Verton, D. (1999). *Serbs Launch Cyberattack on NATO.* Accessible: https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx, 20.11.2018.

Waltz, K. N. (1979). *Theory of International Politics.* New York: McGraw-Hills.

Ward, M. (2018). *Staying one step ahead of the cyber-spies.* Accessible: https://www.bbc.com/news/business-43259900 , 23.10.2018.

Wendt, A. (1995). Constructing International Politics. – *international Security*, Vol. 20, No 1, Summer 1995, 71 – 81.

Wright, Q. (1964). *A study of War.* Chicago, IL, USA: University of Chicago Press.

Zmijewski, E. (2008). *Georgia Clings to the 'Net.* Accessible: https://dyn.com/blog/georgia-clings-to-the-net/ , 20.10.2018.