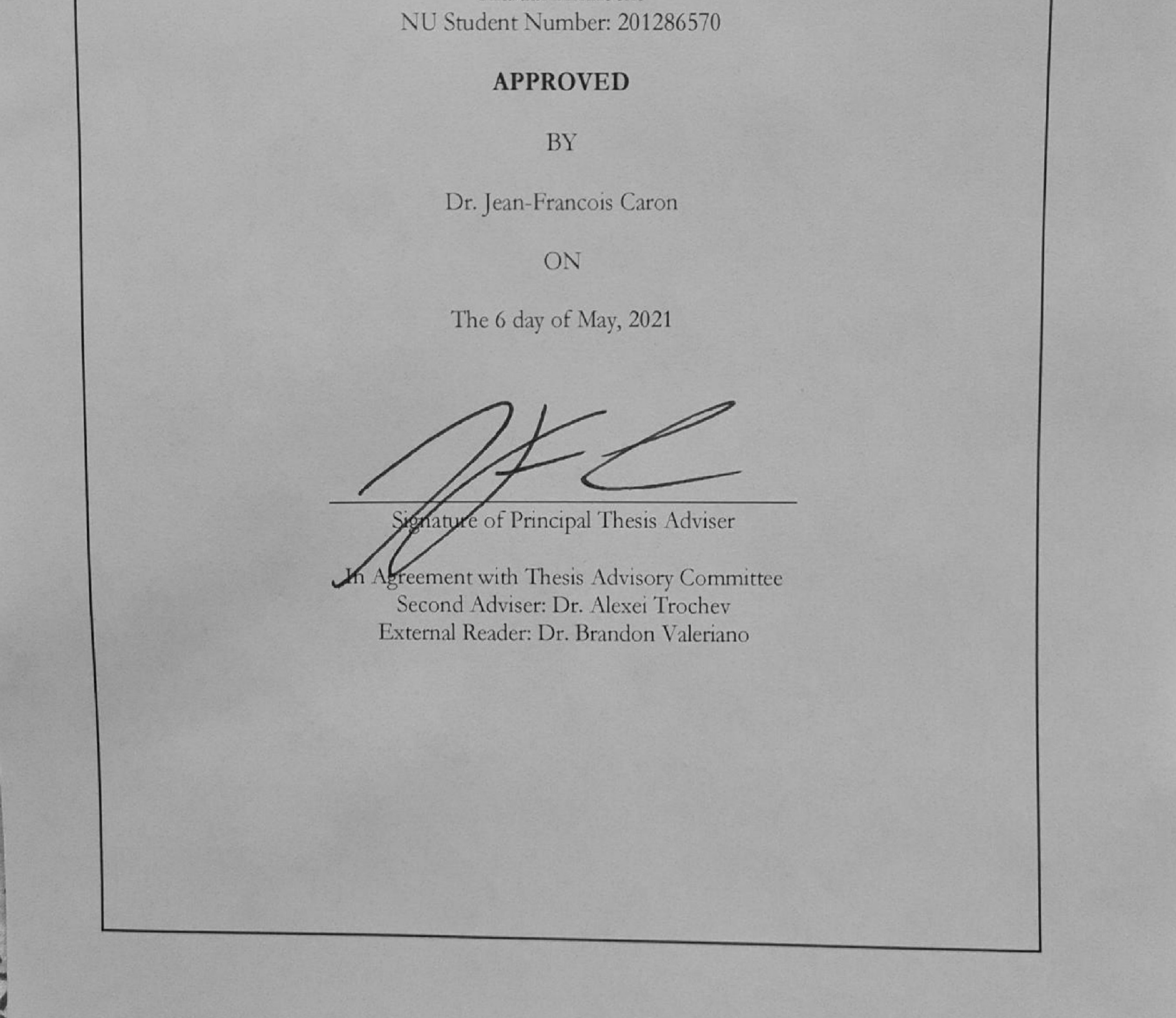

THESIS APPROVAL FORM

NAZARBAYEV UNIVERSITY
SCHOOL OF HUMANITIES AND SOCIAL SCIENCES

CYBERATTACKS AS ALTERNATIVES TO WAR AND ACTS OF WAR
КИБЕРАТАКИ КАК АЛЬТЕРНАТИВНЫЕ МЕРЫ ВОЙНЫ И АКТЫ ВОЙНЫ
СОҒЫС ЖӘНЕ СОҒЫС ӘРЕКЕТТЕРІНЕ БАЛАМА РЕТІНДЕ

BY
Alaidar Amirseiit
NU Student Number: 201286570

APPROVED

BY

Dr. Jean-Francois Caron

ON

The 6 day of May, 2021

Signature of Principal Thesis Adviser

In Agreement with Thesis Advisory Committee
Second Adviser: Dr. Alexei Trochev
External Reader: Dr. Brandon Valeriano

CYBERATTACKS AS ALTERNATIVES TO WAR AND ACTS OF WAR

КИБЕРАТАКИ КАК АЛЬТЕРНАТИВНЫЕ МЕРЫ ВОЙНЫ И АКТЫ ВОЙНЫ

СОҒЫС ЖӘНЕ СОҒЫС ӘРЕКЕТТЕРІНЕ БАЛАМА РЕТІНДЕ КИБЕРШАБУЫЛДАРДЫ ҚОЛДАНУ

by

Alaidar Amirseiit

A thesis submitted in partial fulfilment of the requirements for the degree of

Master of Arts in

Political Science and International Relations

at

NAZARBAYEV UNIVERSITY -

SCHOOL OF HUMANITIES AND SCIENCES

2021

Dedication

I would like to dedicate this MA thesis to my mom, Dinara, for her unwavering support and encouragement throughout my studies. Thank you for everything that you have done.

Abstract

There is an inherent problem with the way the term cyberattack is being used. The term cyberattack is applied to any type of hostile interaction that occurs within cyberspace and presented as either act of war or a criminal act. Cyberattacks are not binary, they represent a continuum of acts both violent and non-violent. Hence, the point of this thesis is to answer *What types of cyberattacks can be classified as non-violent, violent alternatives to war and acts of war?* I develop a classification model that accurately classifies cyberattacks based on the scale and effect of the cyberattack.

The existing literature on cyberattacks presents them as non-violent alternatives to war, as cyberattacks are non-kinetic and existing cyberattacks have not caused deaths of civilians or any level of destruction. However, such a perspective is limited, as cyberattacks have a potential to cause deaths and destruction. I remedy this by discussing what makes non-violent alternatives to war non-violent, and what makes violent alternatives violent. Furthermore, I dive into the consideration of what constitutes acts of war and develop the rule of the 3Ds, which states that for a use of force to be considered as an act of war, it needs to cause significant destruction, significant disruption, and numerous deaths. Based on these considerations, I use the severity scale of the Dyadic Cyber Incident Dataset developed by Maness, Valeriano, and Jensen (2019) to accurately establish thresholds for cyberattacks that fit within categories of non-violent alternatives to war, violent alternatives to war and acts of war. In this research I rely on the cyberattack case of Stuxnet and cyberattack cases derived from popular culture: TV series Homeland and Die Hard 4.0.

TABLE OF CONTENTS

LIST OF TABLES

Acknowledgement

I would like to express my deep gratitude to Doctor Jean-Francois Caron, my primary advisor, for guiding me in this academic endeavor. His encouragement to push on and valuable feedback were crucial in the successful completion of this MA thesis. I would like to also thank Doctor Alexei Trochev, my second advisor, for his advice and assistance in structuring and clarifying this thesis. I really appreciate all the time and energy that these scholars have dedicated to my research project. I would like to express gratitude towards Doctor Brandon Valeriano, whose work on cyberattacks has inspired this research project and whose valuable feedback and constructive comments helped me polish this thesis work.

I want to thank my bosses Gulzhan Bigaliyeva and Nellufer Adai, colleagues: Arailym, Banu, and Aisulu for their support during the production of this thesis.

I want to thank my mom and friends, especially my best and dearest friend, brother-in-arms Olzhas Gibatov and my roommate Cesar Gonzalez-Flores, who supported, encouraged, and assisted me throughout my study.

Chapter 1. Introduction

This thesis is about cyberattacks and the consideration of cyberattacks as a continuum of violent and non-violent actions. There is a problem with the rhetoric surrounding cyberattacks. The term cyberattack has been treated either too narrowly or too broadly. To address this issue, this thesis tries to establish a middle ground between these extremes through the development of a classification that would accurately reflect the reality of cyberattacks and their application.

The narrow interpretation of cyberattacks stems from the consideration of cyberattacks as binary. Policy makers treat cyberattacks as either black or white, as either acts of war or not. This is a faulty representation of cyberattacks. The reason for this is that cyberattacks generate fear of a "Cyber Pearl Harbor" that could potentially disrupt and destroy critical infrastructure. However, this fear leads to the misinterpretation of cyberattacks and generation of false rhetoric. Consider the incident that happened between Russian and Denmark in 2017 (MacFarquhar 2017). In the Denmark case, Russia "hacked into email accounts at Denmark's Defense Ministry" (MacFarquhar 2017). Defense Minister Claus Hjort Frederiksen interpreted this attack as part of "continuing war from the Russian side," even though "the hacked emails don't contain military secrets" (MacFarquhar 2017). This is an act of cyber espionage, which is not considered as an act of war.

> With respect to espionage, states have not found espionage to be a per se violation of sovereignty, even when those actions take pace in and/or have effects in another state. States routinely outlaw the methods of espionage as a matter of domestic law, but not as a violation of sovereignty (Jensen 2016, 742).

Since espionage is not considered as an act of war, cyber espionage follows this logic, and it is dealt with through domestic laws. However, this does not prevent states from generating a sense of "war" within the public consciousness. Rather than a binary phenomenon, cyberattacks consist of various types of actions, which can be classified as violent or non-violent. However, within the scholarly community the understanding of what constitutes a cyberattack is too broad.

The understanding of cyberattacks as being too broad stems from the fact that pretty much any kind of incident that happens within cyberspace is considered as cyberattack. Valeriano and Maness (2015, 211) reflect this fact within their argument

> To be clear of our usage of terms, we have relied on the terms of *cyber incident* and *cyber dispute* to distinguish them from the overuse term *cyber attack.* It is unclear what exactly a cyber attack is, since it now seems to mean everything from a Twitter hack to a full-scale government operation.

For political scientists, like Valeriano and Maness, the term cyberattack is too broad, as a breach of the information system could mean anything. When the rhetoric of war is used alongside any cyberattack, it gains the definition that lends itself to overuse. Hence, considering the fact that cyberattacks have been used in different instances with such a freedom, there is a need to establish a concrete classification that would accurately allocate cyberattacks into respective categories.

Consider the typology, which Caron (2019, 111) proposes. The proposed typology differentiates between cyberattacks based on the considerations of intent, scale and effect and provides the following typology – cyberattacks as

- Constitutive element of full-scale war: cyberattacks are used alongside conventional kinetic attack
- Form of political intimidation/interference: manifestation of disagreement with another country’s policies
- Way to spy on the enemy: cyberattacks as a tool of espionage
- Act of war: cyberattack is launched against military or non-military target with clear intention to produce mass destruction
- Measure short of war: cyberattack as a tool for preventing transgressions of hostile state by causing localized damage to evoke concessions

This proposal accurately depicts the nature of cyberattacks, as it offers a typology of cyberattacks based on the scale and effect. However, the proposal lacks a clear differentiation of measures within the measure short of war category. The differentiation depends on the consideration of equivalent measures within the conventional uses of force. Caron (2019, 112) poses this question by asking about the possible equivalent of drone strike with cyber means. Partial answers can be found within the book of Gross and Meisels (2017).

Gross and Meisels (2017) wrote a book that discusses soft war. Soft war is a term used for the deployment of non-kinetic measures as a way to pressure hostile states to concede and change their behavior. Gross and Meisels (2017) treat cyberattacks as measures of soft war, since they do not use kinetic force to evoke concessions, and no current cyberattack have caused deaths among the civilian population. However, this view is limited. Treating cyberattacks purely as soft war, which I will refer to as a non-violent alternative to war, does not cover all possible cyberattacks. It is true that current cyberattacks are used to temporarily disable systems by causing non-critical damage; however, this does not mean that cyberattacks are not capable of crossing the threshold. They can be a cause of deaths or cause of prolonged and significant disruption of basic human needs. Cyberattacks have capability to cause deaths and widespread disruptions, which can be considered as a violent alternative to war or an act of war depending on the scale and effect of the attack. Therefore, based on the argument of Caron (2019) and the problem within the classification of cyberattacks in Gross and Meisels' (2017) argument, there is a need to fill this gap by asking the following research question: *What types of cyberattacks can be classified as non-violent, violent alternatives to war and acts of war?* To answer this question, first I will offer a definition for cyberattacks and then present the structure of my thesis.

My definition of cyberattacks draws on the portrayal of cyberattacks by Gross and Meisels (2017) and Valeriano and Maness (2015). Specifically, my definition of cyberattacks expands upon the aspect of "specific purpose" within Valeriano and Mannes' (2015, 211) definition. I define cyberattacks as *the use of force that possesses kinetic and non-kinetic capabilities necessary to affect the target with a purpose of evoking concessions from it*. By using this definition, I account for the classification of cyberattacks as non-violent, violent alternatives to war, and acts of war. Within the scope of my thesis, I will consider only coercive cyberattacks, and will omit discussion of cyber espionage and disinformation cases.

The literature review chapter will cover several topics. The first one is concerned with the definition of war. I will look into the definition of war based on the Tallinn manual and specific interpretations of war by various social sciences, like jurisprudence, just war theory, political science and sociology. These definitions are limited and do not offer a detailed perspective on war. Hence, I develop a definition of war based on the considerations of Wolfendale (2017) and certain aspects that are present among several existing definitions of war. The definition includes the satisfaction of the rule of the 3Ds, which are destruction, disruption, and deaths. The rule is based on the effect that act of war produces and the scale of the attack. Afterwards, I present the consideration that cyberattacks are not considered as acts of war, which is true, but this omits the possibility of them becoming one. This can be seen from the Dyadic Cyber Incident Dataset (DCID) which is developed by Maness, Valeriano, and Jensen (2019), Within the dataset they developed a severity scale that portrays the effect of cyberattacks, which can be used as an equivalent for conventional attacks. Based on their dataset I will develop a threshold model for acts of war in the Classification chapter. Furthermore, the chapter elaborates on Gross and Meisels (2017) analysis of cyberattacks as a soft war measure, which I argue is limited and the understanding should be expanded.

The theory chapter covers the nature of non-violent, violent alternatives to war and acts of war. Discussion is based on the analysis of conventional measures and looking into what makes them non-violent or violent alternatives to war based on the discussion of sanctions, embargoes, and diplomatic criticism, as well as targeted strikes and special operations. The reason for asking this is that some non-violent alternatives to war, despite being non-kinetic, cause disruption of basic human needs, which causes deaths among the innocent civilian population, like the imposition of sanctions on Iraq. During my discussion, I arrive at the conclusion that non-violent alternatives to war are non-violent despite causing deaths among the civilian population because these considerations were not included in the decision-making process. This is because these effects were not intentional, and I consider them as collateral damage that may happen during the imposition of sanctions. The discussion on violent alternatives to war is tightly connected to the discussion of acts of war. If a violent alternative to war exceeds the scale and effect of damage, then it could be *casus belli*. Hence, I provide the definition of violent alternatives to war and elaborate the rule of the 3Ds. I explain that the logic behind the rule is that for the use of force to be considered as an act of war it must cause widespread destruction, significant disruption of basic human needs, and be a direct or indirect cause of mass deaths. At the end of the discussion, I develop several hypotheses about which cases can be considered as non-violent and violent alternatives to war.

The classification chapter covers the development of a classification model. The model is based on the consideration of the hypotheses developed within the theory section and the severity scale of cyberattacks in DCID. Upon the analysis of the severity scale, I included a new category, as levels 1 to 3 represent cyber espionage activities. Levels 4-6 are allocated to the non-violent alternatives to war. Cyberattacks that fit within the definitions of levels 7-8 are classified as violent alternatives to war. Cyberattacks that fit within levels 9-10 are considered as acts of war, based on the consideration of the rule of the 3Ds.

The case studies section is concerned with the presentation and the analysis of actual and hypothetical cases of cyberattacks. For the non-violent alternatives to war, I use the Stuxnet attack that was discovered in 2010. It affected the centrifuges in Natanz nuclear plant in Iran, by causing malfunction; thus, temporarily halting Iran’s nuclear program. I consider it as a non-violent alternative to war, as the attack does not cause any deaths and the damage is localized to a single facility. For violent alternatives to war, I choose a hypothetical case derived from the television series Homeland and refer to the case as the Pacemaker hack. The hack is responsible for causing a targeted death of a single individual. I interpret this as being equivalent to a targeted strike. For the act of war, I choose to discuss the plot of Die Hard 4.0, where a group of terrorists conduct a series of cyberattacks called “Firesale,” which cause widespread destruction, significant disruption of critical national infrastructure, and directly and indirectly causes mass deaths. Since, this attack is meant to represent a “Cyber Pearl Harbor,” if it were to happen in real life, then it would be considered as an act of war.

Chapter 2. Literature Review

The whole consideration of cyberattacks as acts of war, legally, is based upon the soft law of the Tallinn Manual, which, in itself, draws its conclusions from the customary international law and international disputes. Tallinn Manual uses international disputes, like the one between the USA and Nicaragua as a basis for the precise definitions that can be used to shape the legal perspective on cyberattacks as acts of war. The case of *Nicaragua v. United States of America* in 1986 helps better understand what kind of operations can constitute an armed attack (Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) 1986). In the Court's judgement the definition of what constitutes an armed attack was established.

> It must considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border , but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (inter alia) an actual armed attack conducted by regular forces, "or its substantial involvement therein…" [as well as] assistance to rebels in the form of the provision of weapons or logistical or other support (Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) 1986, para 195).

From this definition, I can come to the following conclusion that armed attacks besides being an act of force through the deployment of armed groups, are also the breach of sovereignty of another state[1]. In this sense, it is not the armed attack but rather the use of force which effect is comparable to an armed attack by another State. The important part is the "effect," as Rule 71 of the *Tallinn Manual* states

> State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense. Whether a cyber operation constitutes an armed attack depends on its scale and effects (M. N. Schmitt 2017, 339).

Hence, there should be some sort of criteria of effects that would show when a cyber operation raises to a level of an armed attack; however, this is not the case. Point 7 of Rule 71

[1] I refer to cases where a foreign state provides financial, equipment, training support to rebel groups in the state of the interest.

states that “[*Nicaragua* judgement] noted the need to ‘distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms’ but provided no further guidance in this regard,” which means that the set of criteria for determining what effects the cyber operations would have developed and applied to the armed attack or constitute it as an act of war (M. N. Schmitt 2017, 341). However, there is a general agreement among the International Group of Experts that “serious injuries or killing of a number of persons or that causes significant damage to, or destruction of property would satisfy the scale and effects requirement,” meaning that the effect of a cyber operation should cause physical damage to the targeted structure or the people (M. N. Schmitt 2017, 341). Hence, based on Nicaragua judgement and Tallinn Manual cyberattack is an armed attack, when it aims to threaten the independence and sovereignty of a foreign state and has an effect that is similar to a physical attack, like large and continuous disruption of infrastructure functions and/or death of civilian population. Furthermore, scholars, like Valeriano and Maness (2015) and Schmitt (2017), tend to use term cyber operations instead of cyberattacks, as the former depicts a wide range of operations, like espionage, destruction, terrorist act; while the cyberattack refers to a certain type of offensive act that could lead towards destruction and injury. However, the definition of armed attack itself only partially defines an act of war.

There are several explanations to what constitutes a war adopted by various fields of social science. Wolfendale (2017) provides definitions of war derived from various fields. Wolfendale (2017) presents definitions of war from the perspectives of Just War Theory, jurisprudence, political science, and sociology. These definitions serve specific purposes, which make them very limited in their application. Consider the definition within the Just War Theory, which identifies “conditions under which waging war is morally permitted rather than the conditions that define war as such.” This means that the JWT definition of war is focused on justifying the war itself rather providing a description of what war is. Despite the fact that the morality of war should be considered prior to waging it, the definition of war under JWT does not show us the specific aspects that would make a conflict between two parties a war.

The juridical definition of war comes in several variations. First is the consideration of what constitutes an act of war based on the ruling of the Nicaragua case. The Nicaragua judgement does not define an act of war straightforwardly, but one can derive definition from the following considerations of "armed conflicts that are not of the international character" are not considered as a war or initiation of collective self-defense tactics (Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) 1986, para 219). Furthermore, the engagement in hostilities should be declared by the state in order to ask for the assistance from the third party, as well determination of a conflict by the Security Council (Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) 1986, para 235). This definition of war does not hold up to the current status of the international arena. Specifically, the factor of declaration does not necessarily work in the current state of the international arena, where acts of violence and force are done covertly, like terrorist acts, special operations that could be classified as acts of war. Furthermore, the inclination towards interpretation of acts of war being international conflicts excludes domestic acts of violence that spur civil wars and could lead to the potential intervention from the third party. Hence, the definition of war based on Nicaragua judgement is not useful for this thesis.

Second is the consideration of Wolfendale's (2017) presentation of juridical definition. Juridical definition "aims to identify the conditions under which the laws of war apply," which I understand as an aim to bring order to the structure of war. The consideration of the juridical definition of war is not limited there, as Wolfendale (2017) uses the definition of the International Law Association – "armed conflict as occurring when there is 'the existence of organized armed groups' who are 'engaged in fighting of some intensity." The definition of ILA is problematic, as the definition considers fighting of undefined level of intensity. Such consideration is too broad, as "some intensity" does not provide any reference points for the consideration of the use of force. Under this consideration border skirmishes or small armed incidents between states could be classified as acts of war. Hence, this definition is not useful within the context of the current thesis.

There are also combinations of definitions that come from JWT and jurisprudence. Such kind of understanding of war can be seen in the perspective of Brian Orend (2006, 2-3), which is the definition of a just war theorist

> War should be understood as an actual, intentional and widespread armed conflict between political communities . . . War is a phenomenon which occurs only between political communities, defined as those entities which either are states or intend to become states (in order to allow for civil war) . . . Further, the actual armed conflict must be intentional and widespread: isolated clashes between rogue officers, or border patrols, do not count as acts of war. The onset of war requires a conscious commitment and a significant mobilization on the part of the belligerents in question. There's no real war so to speak until the fighters intend to go to war and until they do so with a heavy quantum of force.

This definition has several pitfalls that makes it too narrow. From the first look, the definition seems broad, but it has several factors, like the limitation to political communities and the consideration of a heavy quantum of force. The limitation to political communities omits some non-state actors from the consideration of warring parties. For instance, hacker groups or terrorist groups themselves may not be considered as political communities, but they could initiate a war by hacking a power grid and causing a massive and prolonged blackout or conduct a terrorist act and cause massive deaths. Hence, according to Orend's definition, war is a public and a widespread endeavor between states that should be declared; however, this is factors of war being widespread and public is only part of the definition of an act of war, which should include considerations for the suffering of people and the effect of war on civilians independent of belligerent parties.

Political definition of war “focuses on the aims that characterize the use of war,” as in Clausewitz’s definition of “an act of violence intended to compel our opponents to fulfill our will” (Wolfendale 2017). The classical Clausewitzian definition of war is outdated, as under its considerations even the non-violent uses of force, like sanctions and embargoes would be classified as acts of war, which is an incorrect assumption. Furthermore, the political definition of war also does not provide any criteria for what constitutes an act of war, specifically, what act of force would be considered as an act of war. Instead, the definition focuses on the motivations and goals of war, which is helpful only during an analysis of war in itself, after its initiation and possible after the conclusion of war efforts. Hence, the political definition of war serves the purpose of justifying war rather than showing how war starts.

The closest interpretation of what war is comes from sociology. Sociological definition focuses on the very specifics of war – specific numbers of casualties, preparation and legitimation (Wolfendale 2017). This offers scholars and me an opportunity to understand what war is, i.e., shows the point when a battle between multiple warring parties becomes a war – 1000 deaths per month on the battlefield. However, this is where Wolfendale (2017) disagrees with the definition, as the use of specific numbers of casualties makes the difference between “war and lesser conflicts” arbitrary. I agree with her critique, as the consideration of specific number of casualties on the battlefield does not take into consideration the possible suffering of civilians. The consideration of this effect can provide an explanation for “when and why a conflict becomes a war” (Wolfendale 2017). If an armed attack causes a serious suffering of civilians, either physical or psychological, then the attack can be considered as an act of war. For instance, consider a situation where a terrorist organization hijacks a control tower of an airport, and makes several planes crash into each other, which can be conducted using cyberattacks. This attack is both public and inflicts serious suffering on civilians both the passengers of the plane and their relatives. Furthermore, the attack or use of force should possess the aspect of disruption of access to basic human needs for civilian population (Wolfendale 2017). The disruption of basic human needs provision better shows an impact that act of war has on the daily lives and securities of the innocent civilian population. The significant disruption of the provision endangers the lives of civilians, bringing them into the war effort and forcing them to be part of the war effort. Therefore, an act of war should possess three characteristics:

1. Act of war should cause mass destruction of property.
2. Act of war should cause a significant disruption of provision of basic human needs.
3. Act of war should cause massive deaths among the civilian population or members of the military.

Hence, the definition of the act of war is the use of force that causes widespread destruction, significant disruption of basic human needs and cause of massive deaths (direct and indirect), which I present as the rule of the 3Ds: destruction, disruption and deaths as results of the use of force.

The consideration of these factors points towards the fact that cyberattacks in their current iteration are not considered as part of a conventional war. Current cyberattacks, when conducted, are public and do not cause serious injuries to the civilian population. Cyberattacks are public, but they typically consist of deniable actions as their deployment occurs behind the closed doors in a much more private environment, and mostly constitute covert operations rather than open declarations of intention. The result of the cyberattack can be left unnoticed unless either a spillover effect happens, i.e. the attack starts to affect civilian population, or states decide to disclose that they have been attacked. Furthermore, cyberattacks are yet to cause serious injuries to the civilian population, as attacks, such Stuxnet, Wannacry, NotPetya, or attack on the Ukrainian electrical grid did not cause death or severe psychological trauma among civilian population. Hence, the scale and effect of the current cyberattacks is not enough to cross the threshold of war. As a result, with the lack of concrete cases for the assessment of cyberattacks as acts of war, the term has been difficult to apply to the framework of *jus ad bellum*, as well as justify them as acts of armed attacks, which could be considered as acts of war. However, this does not mean that cyberattacks cannot be considered as acts of war. Valeriano and Maness (2015, 31) mention Nye's (2011) definition of cyber warfare as "hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence." I do not agree with the use of the term "cyber warfare," as cyber violence would better fit this particular description. I do agree with the equivalence of cyberattacks with kinetic violence. There can be cases where cyberattacks have effects that are comparable to an act of war, like the hacking of an airport control tower and making planes crash into each other.

Maness, Valeriano, and Jensen (2019) developed a Dyadic Cyber Incident Dataset, which uses the severity scale as one of the criteria. The dataset itself is based on the analysis of 266 cases of cyberattacks that occurred between 2001 and 2016, which are categorized based on the state, interaction, severity, concession, involvement of third parties and type of target. This is a much fuller dataset compared to cyberattack dataset compiled by Council of Foreign Relations, which covers a greater time period but does not cover all of the cyberattacks (Tracking State-Sponsored Cyberattacks Around the World n.d.). I compared the number of cyberattacks, where the U.S. was the initiator of the attack. DCID has 103 cases, where the U.S. conducted cyberattacks against other states. Dataset of the Council of

Foreign Affairs shows only 15 cyberattacks initiated by the U.S. (Tracking State-Sponsored Cyberattacks Around the World n.d.). Another point of interest in the dataset besides the collection of cases of cyberattacks is the inclusion of severity scale. This scale is rated from 0 to 10, where 0 is absence of cyber activity and 10 is massive deaths from the cyberattacks (Maness, Valeriano, and Jensen 2019, 7–8). The scale provides a very accurate representation of the scale and effect that current, and potential cyberattacks might have. Therefore, based on the considerations of the dataset, cyberattacks can also be considered as either non-violent alternatives to war (Stuxnet and localized destruction of centrifuges), violent alternatives to war (pacemaker hack, which causes death of its user) or act of war (widespread destruction and significant disruption of critical national infrastructure and deaths among civilian population).

The main reason for not considering cyberattacks as a violent alternative to war is the fact that existing cyberattacks are non-lethal, which makes them non-violent. Gross and Meisels (2017) claim that cyberattacks should be considered as a "soft" alternative to war.

> Soft war is non-kinetic war. Bytes, boycotts, propaganda, nonviolent resistance, and even kidnapping replace bullets and bombs and supplant the predominant role of lethal force that captures or images of war. Unarmed force is not deadly but it is also not passive. It may be soft to the touch but is as coercive as any act of terrorism or targeted killing. <…> Hard war is kinetic: bombs, bullets, and missiles; its outcomes are death, injury, and devastation. Hard war is the chief concern of the international law and moral philosophy (Gross and Meisels 2017).

Soft war compared to hard war is conducted without using bullets but by applying political and economic pressure, which evokes concessional changes in hostile states. Soft war measures do not use kinetic force to afflict states, as the state using soft measures applies pressure to certain sectors without causing deaths, like the hard war measures, which include the consideration of deaths within the justification of deployment of measures. The applied pressure comes from the economic limitations or ban on selling and buying arms, as well as application of diplomatic pressure through the deterioration of diplomatic relations. Gross and Meisels (2017) consider economic sanctions, arms embargoes, diplomatic criticism, and cyberattacks as measures of soft war. "Cyber conflict of one type should be included within the purview of "soft" or "unrestricted" warfare," which is "state-sponsored hacktivism" (Lucas 2017). Cyberattacks and especially state-sponsored hacktivism have not caused any casualties among the civilian population. Cyberattacks have been the cause of defacement of websites and the crash of governmental facilities, but the damage was not enough to cause severe injuries to civilians' bodies or minds. Hypothetically, there could be a cyberattack that will disable the electric grid or damage a nuclear reactor to the point of meltdown or a situation where the hacking of a control tower results in a crash of several planes; however, these all are hypothetical cases, which were not reproduced in the real world. Hence, since cyberattacks have not caused kinetic harm, they are considered as non-violent alternatives to war seems to be more suitable; however, adopting the position that cyberattacks are non-violent alternatives to war only completely ignores the fact that cyberattacks are also violent alternatives to war.

The consideration of cyberattacks as violent alternatives to war is not well discussed within the literature. The major works on cyberattacks, like Valeriano and Maness (2015) use the term cyber conflict and refer to cyber war and focus specifically on cyber conflicts between dyadic rivals. Gross and Meisels (2017) discuss the non-violent alternatives to war and provide a comprehensive analysis of those to identify the role of non-violent alternatives to war within contemporary warfare. Furthermore, there seems to be a vagueness in the definition of cyberattacks. Nye's definition of cyberwarfare is a prime example. "Hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence" (Valeriano and Maness 2015, 31). This definition poses a problem, as it does not provide a clear distinction between scale and effect of acts of violence and acts of war. It creates a confusion when one tries to provide a distinction between different type of cyberattacks and their effects. For the purpose of this thesis, cyberattacks as violent alternatives to war would include cases, where as a result of an attack people die, as within targeted strikes; while acts of war by cyberattack would include cases like remotely hijacking an airplane to make it crash into another plane or a building. Hence, there is a need for the development of a comprehensive typology that would clearly distinguish between non-violent, violent alternatives to war and acts of war. Doing so requires an approach that considers all the possible aspects of cyberattacks. The non-violent alternatives to war are being analyzed through the pragmatic approach developed by Pattison (2018).

The model for the analysis of non-violent alternatives to war is developed by Pattison (2018). The approach used by Pattison (2018) complements the arguments developed within Gross and Meisel's (2017) book, as the pragmatic approach provides a justification for reasons "soft" measures are used. Pattison (2018, 18) uses a pragmatic approach for the analysis of the alternatives to war, like sanctions, embargos, diplomacy, positive incentives. The argument is that a pragmatic approach helps determine, whether an alternative should be launched because it is better than doing nothing, and whether the alternative is better than other measures (ibid). Pattison (2018, 28-29) develops a model of justification which is based upon five values of effectiveness, fairness, distinction between doing and allowing harm, mediation of harm, and desert. The core attributes of the pragmatic approach are the consideration of likely features and effects of alternatives, offering of an ethical account of alternatives both in ideal and nonideal features of the international system, and the consideration of the effectiveness as the most important measure. The consideration of likely features entails the consideration of relative effectiveness of alternatives. Pattison's (2018) analysis offers an in-depth consideration and justification of the deployment of "soft" alternatives to war, like sanctions, embargos, diplomacy, and positive incentives, as the considerations that he offers are based within nonideal circumstances of the real world. This means that the consideration of whether to deploy the measure or not could be derived with the consideration of "lesser of two evils." For instance, sanctions are not always effective and may result in the suffering of innocent civilians; however, since they sometimes bring more good than harm policymakers resort to sanctions. Hence, it is possible for the policymaker to consider imposition of sanctions and allow harm to the civilian population, under the condition that afterwards the general situation of human rights will be better. This approach can be used as an analytical basis for the justification of cyberattacks as non-violent alternatives to war. However, there are other approaches that were used by scholars to analyze cyberattacks. The consideration of approaches has been a widely debated topic when it comes to the justification and analysis of attributes of war.

The debate itself is driven by the effect-based analytical approach, which is a parsimonious version of the Pragmatic approach. As it was stated in the *Nicaragua* judgement and the Tallinn Manual, effects determine whether an attack is an armed attack and validates the exercise of the inherit right to self-defense. Hence, the effects-based approach can be understood as an analytical approach that focuses on the effect that a particular measure produces. The pragmatic approach that Pattison uses is a more advanced version of the effect-based approach, as besides the consideration of the effect of measures, Pattison also considers moral aspects of alternatives, while the pure effect-based approach focuses on the success of the deployment of alternative measures. However, it is not the only analytic approach, as there are instrument based approach, target-based approach, absolutist and idolized approaches (Pattison 2018, 30–31; Roscini 2014, 46–47).

The instrument-based approach and the target-based approach are not viable approaches for the analysis and justification of "soft" measures. The instrument-based approach, which Roscini adopts in his chapter, "focuses on the means used to conduct an act, i.e. weapons, and has been traditionally employed to distinguish armed force from economic and political coercion" (Roscini 2014, 46, 49). However, the instrument-based approach does not account for the cyber weapons, as they do not possess the physical characteristics that conventional weapons would. Another interpretation of the instrument approach is Pattison's "fully instrumentalist approach," which considers only the efficiency of deployed measures and based on that consideration the decision to deploy or not to deploy is made. Such an approach ignores other values, such as fairness and desert, and lacks the moral considerations. The target-based approach, on the other hand, is "overinclusive" as under its consideration, even a small manipulation of data in national critical infrastructure would be considered as a use of force (Roscini 2014, 47). The absolutist and idolized approaches look similar to each other, as they consider the ideal moral circumstances under which a measure can be deployed. These approaches are not considered because there is no consideration of nonideal circumstances. For instance, the imposition of sanctions or arms embargoes can lead to the suffering of people, while punishing the people that deserve to be punished and lead to the eventual development of a state. Based on the consideration of approaches, the pragmatic approach offers the best basis for the analysis and justification of cyberattacks as non-violent alternatives to war. Since, Pattison (2018) does not talk about or even mention cyberattacks, this offers me an opportunity to contribute to the literature and develop a typology that comprehensively differentiates cyberattacks as non-violent, violent alternatives to war and acts of war. Hence, the question that I am interested in can be formulated as *what types of cyberattacks can be classified as non-violent and violent alternatives to war and acts of war?*

Table 1. Analytical Approaches

Approach	Key elements
Pragmatic Approach	consideration of likely features and effects of alternatives, offering of an ethical account of alternatives both in ideal and nonideal features of the international system, and the consideration of the effectiveness as the most important measure
Effect-based Approach	focus on the effect that a particular measure produces
Instrument-based Approach	focus on the means used to conduct an act, and its efficiency
Target-based Approach	Overinclusive – a small manipulation of data in national critical infrastructure would be considered as a use of force
Absolutist Approach	No consideration of the non-ideal circumstances
Idolized Approach	

In conclusion, there are many attempts to situate cyberattacks within a specific realm of either war or measures alternative to war, but they are all short of accomplishing this goal. The consideration of cyberattacks as an act of war does not cross the threshold of being a cause of mass suffering of people, both physical and mental, as well as not being widespread or public, as the conventional wars have always been. The consideration of cyberattacks as a violent alternative to war is underdeveloped within the literature as there is no concrete criteria for the consideration of cyberattacks as an alternative to war or an act of war. Nye defines cyber warfare in a very broad term that includes cyberattacks that are not acts of war, as Ney does not specify the scale and effect of "hostile actions in cyberspace" (Valeriano and Maness 2015, 31). Hence, there is a need for a clear typology that would provide clear criteria for the consideration of scale and effect. To analyze it, I refer to the consideration of cyberattacks as non-violent or "soft" alternatives to war. Gross and Meisels (2017) and Lucas (2017) consider cyberattacks as "soft" measures, as cyberattacks have caused neither casualties, nor severe suffering of civilian population. I refer to this specific research, as it is complemented by the pragmatic approach. Hence, in order to do so, I will use the approach that Pattison (2018) developed to analyze and come up with criteria for when different types of cyberattacks are deployed. This approach considers not only the effectiveness of measures but also the moral value of alternatives, and comparison to other measures and doing nothing.

Chapter 3. Theory

The classification of various real-life and hypothetical cyberattacks as non-violent alternatives of war, violent alternatives to war, or acts of war requires a complete understanding of what makes non-violent, violent alternatives to war. I gain this understanding through the discussion of non-violent alternatives to war (NVAW) and violent alternatives to war (VAW). The understanding starts with intent of the attack, which, in the context of alternatives to war is to affect the policy of the state and reduce the chances of escalating to war. Once this understanding is set, I can discuss the nature of NVAWs and VAWs. What makes non-violent alternatives to war non-violent? What makes violent alternatives to war violent and why are violent alternatives to war are alternatives and not war? I argue that non-violent alternatives to war are non-violent because they do not use kinetic force to coerce hostile states into changing their behavior, but rather apply pressure economically and diplomatically. NVAW coerce hostile states through coercive means, which include but not limited to sanctions, embargoes, diplomatic criticism, and cyberattacks. Violent alternatives to war are violent because they utilize kinetic force in the attempt to coerce the hostile state to change their policy. Hence, this chapter will proceed as the following.

First, I will discuss the nature of non-violent alternatives to war based on the arguments of Gordon (2017), Gross and Meisels (2017), and Pattison (2018) to properly discuss all of the aspects of the NVAWs. Specifically, I will focus on the discussion of what makes NVAWs non-violent, even though they can cause physical damage that leads to the death among civilian populations. Furthermore, the discussion of NVAWs will also include the consideration of their effectiveness once they are deployed from the perspective of statistical research. Second, the consideration of VAWs depends on the consideration of the scale and effect of the attack, as when the attack crosses the threshold of the damage or disruption caused, VAW becomes an act of war.

Non-violent alternatives to war

The nature of non-violent alternatives to war depends on the consideration of whether the deployed measure is non-kinetic. I, along with Gross and Meisels (2017) and Pattison (2018), consider economic sanctions, arms embargoes, and diplomacy as non-violent alternatives to war, as these measures fit under the criteria of non-kinetic coercion and the intent to change the policy of a hostile state to avoid war. To better understand the non-kinetic aspect of non-violent alternatives to war, consider the following two citations:

> Soft war is non-kinetic war. Bytes, boycotts, propaganda, nonviolent resistance, and even kidnapping replace bullets and bombs and supplant the predominant role of lethal force that captures or images of war. Unarmed force is not deadly but it also not passive. It may be soft to the touch but is as coercive as any act of terrorism or targeted killing (Gross and Meisels, 2017).
>
> [Economic sanctions] were considered “peaceful” not because economic sanctions are purported to do no material or human damage, but because sanctions are placed in comparison with “actual war.” From their origins as a curious combination of the “peaceful” and the “deadly,” economic sanctions have come to be seen as a middle route, something more substantial than mere protest or denunciation, yet not violent, in contrast to military intervention (Gordon, 2017).

There are two points that need to be addressed from these citations. First is the consideration of "deadliness." Gross and Meisels (2017) claim that NVAWs are not deadly, as the consideration of deadliness is associated with violence and violent alternatives to war. Hence, how is it possible that Gordon (2017) considers sanctions "deadly"? I consider the aspect of deadliness as a possible side effect of implementation of sanctions and not as a direct result of them. Sanctions by their nature are peaceful alternatives to war; however, their implementation can be mishandled by the hostile government, whose mishandling can lead to deaths among the civilian population. While the violent alternatives to war already include the assumption of death among the civilian population in the process of justifying deployment of violent alternatives to war. Hence, what makes non-violent alternatives to war as non-violent is the absence of intention of harm to the civilians. NVAWs do not intend to cause grave harm to civilians, but only intend to pressure and coerce the hostile government into changing their policy.

Second, both citations point towards one common denominator of NVAW being "peaceful" yet "not passive" entailing that NVAWs can cause as much "damage[2]" as military intervention or targeted killing without resorting to the physical expressions of force. While the violent alternatives to war focus on the utilization of kinetic force to create a localized destruction of a certain infrastructure or facility, non-violent alternatives to war systematically attack a variety of structures and systems that affect the livelihood of states. This creates multiple points that pressure incumbent hostile governments to adopt changes to their policies. For instance, economic sanctions affect the economy of the state by limiting its trading capabilities, which affects the distribution and redistribution of resources for the civilian population. Hence, the main differentiating characteristic between non-violent and violent is that non-violent alternatives to war do not use kinetic force to coerce governments into changing policies and do not intend to cause deaths among civilian populations. Now, I will consider different manifestations of NVAWs from the perspective of how they adhere to the absence of intention to cause deaths.

Economic sanctions are the most well-known case of non-violent alternatives to war, which generates certain moral problems associated with causing harm to the innocent civilian population. The number of studies has been done with the relation to the effectiveness of sanctions (Bapat et al. 2013; Hultman and Peksen 2017; Vines 2012). Economic sanctions are non-violent alternatives to war, as they do not intentionally cause deaths among the civilian population.

[2] By "damage" I refer to the scale of disruption and harm NVAW can cause.

> Economic sanctions are a paradigm case [of non-violent alternatives to war]. One reason for resorting to economic measures rather than full-scale war is "to provide a first, mild stage in the hostilities, to bring moderate pressure to ear to achieve a settlement, if possible, before the resort to arms becomes necessary. <…> Sanctions fulfill an initial, preferably alternative, measure, to be exhausted before reaching the point of last resort [to war] (Gross and Meisels 2017).

However, there are cases when the economic sanctions result in the civilian deaths, which negatively affects their consideration as non-violent alternatives to war and their subsequent deployment justification. At the moment, I will focus on the criticism of sanctions, as criticism makes a case for sanctions to be classified as *violent alternatives to war*, which is a misunderstanding and the misrepresentation of sanctions.

Economic sanctions are double-edged sword that balance between being considered as violent and non-violent alternative to war. The purpose of imposing them is to coercively change the domestic and foreign policies of a hostile state by imposing economic restrictions. Imposition of the restrictions spurred a debate within the scholarly community and general public. The arguments for considering sanctions as violent alternatives to war revolve around the perception of civilian people dying suffering from the imposed sanctions, as well as the fact that imposition of sanctions resemble "siege warfare" (Gordon 2017; Pattison 2018). Such interpretation stems from the assumption that sanctions directly cause deaths among innocent civilian population. The paradigm case of the argumentation are the sanctions imposed on Iraq in the aftermath of the War in Kuwait in 1991.

> The comprehensive sanctions regime against Saddam Hussein's Iraq, in particular, was widely seen as morally reprehensible, and it has been (wrongly) claimed that it led to the death of 500 000 children under the age of five (Pattison 2018. 40).

The reason for such criticism is that "the proceeds from the sales of oil were widely misappropriated, with much of the proceeds not reaching the suffering Iraqi people" (Pattison 2018, 41). In this sense, "economic sanctions are sometimes a trivial interference with business, causing little more than inconvenience. In other circumstances, the effects of sanctions are indistinguishable from those of siege warfare" (Gordon 2017). The circumstances surrounding the sanctions regime in Iraq do resemble the siege, as the sanctions were not the only restriction that was put in place.

The interpretation of sanctions as violent alternatives to war directly points at the flaws of the sanction regime. One of such flaws is presented through the argument of "the indiscriminate objection," where "sanctions are impermissible because they are indiscriminate in that they impose significant harm on those who are not liable" (Pattison 2018, 43). The main problem with sanctions is that they seem to violate the principle of non-combatant immunity, which states civilians should not be intentionally targeted during the war. Furthermore, critics of sanctions claim that imposition of sanctions regime can result in increased repression, that in itself decreases compliance with women's rights, worsen public health and reduces press freedom (Pattison 2018, 43–44). The presentation of sanctions through this perspective presents a picture, where sanctions do more harm than good, as sanctions do not tend to affect hostile policy makers but rather civilian population by either killing them or causing harm. This is not entirely true, as the criticism of indiscriminate objection does not universally render sanctions as unfair or unjust. Sanctions can still be used under certain moral considerations and be effective.

The objection to this criticism would be the consideration of intention to harm the civilian population. The imposition of significant harm on the innocent population is not a direct result of the imposition of sanctions, but the effect of policies in the response to sanctions. In the case of Iraqi sanctions, the government of Iraq at the time did not distribute resources gathered from the "Oil for food" program to its citizens. The resources were distributed to the military to strengthen it. The result of this decision was a massive number of casualties among the civilian population. Sanctions as a standalone measure do not cause deaths among the civilian population. To further ensure compliance to this intention states have adopted smart sanctions, which affect specific individuals or systems without causing casualties among civilian population. Therefore, sanctions are considered and treated as non-violent alternatives to war or as measures of soft war. These measures do not intend to cause casualties among civilian population. This gives a possible hypothesis for a measure to be considered as a non-violent alternative, it should have an intention and act upon it to isolate the damage to a specific target. However, sanctions are not the only non-violent alternative to war. I will now discuss the arms embargo and diplomatic measures, such as naming and shaming.

The arms embargoes are non-violent alternatives to war, as they do not use kinetic force to coerce hostile states. Arms embargoes are a type of sanctions that prohibits state and non-state actors from possessing weapons. Arms embargoes do not directly lead to casualties among the civilian population, which makes it a non-violent alternative to war. Therefore, there are several reasons for the attractiveness of arms embargoes as a measure alternative to war.

The arms embargoes seem to be more attractive than sanctions for several reasons, which do not make arms embargoes a perfect measure. Reasons are reduction of intensity, clean hands argument, small cost of imposition, and, most importantly, more fairly distributed. The reduction of intensity of the conflict happens through the reduction of the means by which combatants fight with each other (Pattison 2018, 72). Thus, the reduction of means also implies that there might be reduction in the duration of the conflict, as the cost of fighting rises for both sides. The argument of clean hands refers to the fact that sender states or states are actively condoning the conflict that is going on within the territory of another state. This serves a very efficient way of not only punishing a hostile state but also signaling to other states that the sender of the embargo is clearly against; even though the sender state might be selling the weapons to the warring parties in secret. The fair distribution of burden takes place because the affected population are those that work directly in weapons manufacturing and selling. Under the consideration of just war theory, those who are contributing to the war effort are stripped off their noncombatant immunity; however, they are stripped off only when they are working within the weapon manufacturing factories. Indeed, this part of the population will be affected even after they exit the weapon manufacturing facility but, since only a small portion of the population is affected the imposition of arms embargoes seems to be more morally justifiable and attractive for the deployment. This is not entirely the case, as the imposition of arms embargoes has major objections.

Just as arms embargoes seem to be morally attractive to the sender, this measure is criticized for several reasons. Embargoes are ineffective, they are used to avoid more serious actions, and create obstacles for freedom fighters. The argument for ineffectiveness stems from the considerations of noncomplying to embargoes both by the sender and the recipient states. "Senders may have an interest in propping up an ally [or] sell arms for financial reasons" (Pattison 2018, 75). States that initiate arms embargoes might be the same states that sell weapons to the recipient states. Hence, it is uncommon to see that sender states covertly provide weapons to the rebels or the governments where the conflict is taking place. "By arming the embargoed state, the sender can reap substantial economic and strategic benefits, which outweigh the consequences of the failure of the embargo of the state (ibid). Furthermore, the recipient state can also receive weapons through covert operations or smuggling through borders making the arms embargo ineffective. Arms embargoes are also criticized for being a "fig leaf" and preventing freedom fighters or legitimate governments from defending themselves. The argument of fig leaf is that arms embargoes are used by states to avoid taking more serious actions. "It gives the impression of 'doing something', thereby potentially quelling domestic demands for action in response to mass atrocities or aggression, without necessitating costly action" (Pattison 2018, 76). Pattison (2018, 76) argues that the plausibility of this objection depends on the presence of more effective and morally acceptable measures. If the arms embargoes are chosen over sanctions or diplomatic measures (like naming and shaming), which would be more effective but costlier, then, indeed, arms embargoes are a fig leaf. However, if the arms embargoes are chosen over measure like war or military intervention, then arms embargoes are the only plausible choice. Furthermore, arms embargo is a complementary measure that should be used alongside other measures, like sanctions.

While the ineffectiveness and fig leaf objections make sense logically, the creation of obstacles to the just movement to fight makes less sense. The argument states that "arms embargoes prevent legitimate states and just rebel movements from defending themselves in the face of unjust attacks" (Pattison 2018, 77). Freedom fighters and legitimate governments cannot protect neither themselves nor others from the attacks, which makes the application of arms embargoes less justifiable. However, this is not entirely true. In cases where there is a clear case of one side being justified to have arms, the arms embargoes could be partial. Furthermore, there are cases where the determination of the just side is impossible, and provision of the partial arms embargo is implausible. It is implausible because then the objection shifts from stopping the hostilities and preventing any further harm done to civilians to supporting a side until it wins in the conflict. This shift cannot be morally justified and the primary objective of keeping civilians safe should be kept. The objections to the arms embargoes do not make much sense, since none of them are solid objections that cannot be overcome. However, this is not to say that arms embargoes are ideal non-violent measures, but arms embargoes are measures that can be effective under certain conditions.

Arms embargoes are the most effective when they are used in conjunction with other measures. The primary objective of non-violent measures is to have an effect on basic human rights. But the arms embargoes influence adherence to the basic human rights by coercing the hostile state to change their policies both foreign and domestic. The arms embargoes are still effective but not all the time. Arms embargoes are the most effective when "they are multilateral, which helps to reduce the flow of arms and strengthen the symbolic sense of disapproval, <…> [also] when [arms embargoes] are used alongside other measures, such as comprehensive sanctions" (Pattison 2018, 89). Furthermore, the most appropriate target for the arms embargoes are the non-state actors, as state actors can counter embargoes (ibid). Hence, arms embargoes can be adopted as complementary measures to other non-violent alternatives to war, which can be applied in a partial manner to affect a specific target without causing suffering to the civilian population. These examples of non-violent alternatives to war serve as one of the most common and prominent choices for politicians as tools of public diplomatic coercion that use economic force. However, there is another less forceful but still impactful measure that I need to discuss, which is diplomacy.

Diplomacy is a multifaceted tool that mostly affects the reputation of a hostile actor. Diplomacy when used against hostile states, in the form of naming and shaming or deterioration of diplomatic ties, affects their reputation by harming it. To better understand where the diplomatic measures stand relative to sanctions and embargoes, I will make the following examples of when the measures are used. Diplomatic measures are the first line of non-violent measures, as they serve as a warning for the hostile states. If the hostile state continues to disregard human rights or threaten the sovereignty of another state, then the international community engages in harsher measures, such as imposition of sanctions along with arms embargoes. This does not mean that if diplomatic measures do not result in changing the policy and behavior of the hostile state, then diplomatic measures should be abandoned. Diplomatic measures should be used as a standalone measure and along with other measures like sanctions or arms embargoes, or the violent alternatives to war. The diplomatic measures, such as naming and shaming are not perfect measures but they help influence the actions of the international community in several directions.

Diplomatic criticism or "naming and shaming" is an effective measure for moral and economic reasons. The moral reasons include the addressing of issues, contribution to global norms, and the wide use. The economic reason includes only one consideration – the cost of imposing such measures on a hostile state, as the application of diplomatic criticism does not carry economic losses, unless states decide to sever the diplomatic relationship between condoning states and hostile states. I draw these considerations from Pattison's book (2018) as his analysis and justification of the non-violent measures short of war are drawn from the perspective of objective analysis with the consideration of both advantages and drawbacks of measures. I agree with his points about diplomatic criticism but with minor additions. Pattison (2018, 92) lists addressing the issue as an advantage of diplomatic criticism. Author argues from the point of constructivism and the desire of a state to "seek (perceived) legitimacy." "When states are criticized, challenges are posed to their reputations and their international standing" (Pattison 2018, 92). This argument stems from the fact that states care about their standing on the international arena, and the subsequent loss of that standing will result in economic losses and issues with self-identity – the wrong perception of self as "force of good." While it is true that states care about the perceived legitimacy, the losses are marginal in the contemporary world. For instance, if previously, the diplomatic criticism was coming mostly from the Western block, after the collapse of the Soviet Union, with the rise of China, diplomatic criticism coming from the Western block is less prominent. The reason is that naming and shaming, while bringing attention to the issue, results in lower pressure in the contemporary since the loss of reputation or in economic gains is relatively small. China is ready to provide economic assistance to the states that are boycotted by the international community. They do it mostly from the perspective of the economic gains, as they lend money to the states with low international reputation. Hence, the naming and shaming becomes problematic. Pattison (2018, 95) states that there are states, which are completely delegitimized, like Syria and North Korea, to whom application of diplomatic criticism applies very little pressure. However, this is not to say that diplomatic criticism does not work. Diplomatic criticism works if we consider the argument of interests. The interests of states are not fixed and are subject to change; hence, the application of diplomatic pressure may yield results if the hostile state is open to the persuasion.

The diplomatic criticism contributes to the global norms by signaling that norms are broken and reinforces the idea that the norms should be upheld. Condoning states through the diplomatic criticism signals the hostility of the targeted state, that it has broken certain norms that exist on the international arena. Furthermore, a diplomatic criticism assists in justifying certain measures, as measures, like sanctions or arms embargoes, are implemented in support of a violated norm (Pattison 2018, 96). Indeed, the application of diplomatic criticism helps in supporting certain norms, like breach of sovereignty or annexation, and reinforces the idea that "morally valuable law *is* law" (Pattison 2018, 97). However, this is only one side of the argument, as there are cases, where the condoning and criticism are not supported by other states. The case of China not particularly caring about the violation of norms and may still continue supporting a hostile regime, since that hostile regime provides certain regional and economic advantages, like infrastructure projects that China has initiated in a number of states located in Africa. Consider, the condoning of Russia's annexation of Crimea in 2014. "Brazil's failure in 2014 to condemn Russia for annexation of Crimea not only reduced reputational costs on Russia, it also weakened the sense that annexation of another state's territory is perceived impermissible" (Pattison 2018, 97 – 98). Hence, the following argument can be made. Diplomatic criticism, indeed, helps reinforce the idea and legal weight of norms, but its effectiveness depends on the collective perception of norms. A state, like China or Russia, may not condone certain actions; thus, as in the example of Brazil, state reduces the weight of the norm, making it ineffective. Moreover, states may choose not to condone certain transgressions based on their perception of the relationship between a government of a hostile state and the insurgent groups. For instance, a civil war is going on in a state, the US is supporting an insurgent group and issues a diplomatic criticism. The US is supported by the NATO allies and allies in Asian region. Russia and China are in support of the acting government of the hostile state and do not support the diplomatic criticism. They will not support the initiative launched by the US making the diplomatic criticism less impactful, as not all the states are sharing this perception of insurgent groups being freedom fighters. Therefore, diplomatic criticism is not a foolproof measure and depends on the collective perception of norms, which can be undermined. Still, the diplomatic criticism is an appropriate first step in the consideration of measures to change the behavior of the hostile state. It signals to the international community that the actions performed by a hostile state should be condoned and hostile states should be punished for them. Based on this, I can formulate the following hypothesis: an appropriate non-violent alternative to war should shed light on the transgressions that a certain state has performed to the international community. Furthermore, it should not be dependent on the constructivist perspective and should effectively change the behavior of a hostile state.

The case of cyberattacks presents an interesting avenue for the consideration of NVAW. Under the consideration of soft war, cyberattacks are considered as tools of soft war, as they do not utilize kinetic force and as result of cyberattacks do not kill people. There are multiple uses for cyberattacks.

> “Soft war” (or “unarmed conflict”), by analogy, is a comparatively new term designating actual warfare tactics that rely on measures other than kinetic force or conventional armed conflict to achieve the political goals and national interests or aspirations for which wars are always fought (Lucas 2017).

However, not all the instances of cyberattacks will fall under the considerations of NVAW. For instance, cyberattacks that coerce the hostile governments into changing their policies can be considered as NVAWs. Cases of cyber espionage and disinformation, on the other hand, will not fall under the consideration of NVAW. Jensen (2016, 742) argues that cyber espionage is not "a per se violation of sovereignty, even when those actions take place in and/or have effects in another state" as cases of cyber espionage are "routinely outlawed as a matter of domestic law, but not as a violation of sovereignty." Hence, cases of cyber espionage exist within their own separate category, which is not covered by NVAW. When considering cyberattacks as NVAW, Lucas (2017) tackles the issue of state-sponsored hacktivism, which describes acts like "straightforward crime and vandalism to many forms of political protest carried out on the Internet". He considers cyberattacks as measures of "soft war," because they can do the same amount of pressuring the hostile states to evoke concessions as conventional attacks.

> Why bother to pursue the risky and wantonly destructive traditional strategic objectives of conventional warfare that Clausewitz describes as "destroying the enemy's army, occupying his cities, and breaking his will to resist" when the strategic objectives can be met instead by rendering the enemy's armies inoperable and non-functional, bringing his cities' commercial and civil activities to a standstill, and forcing his military leaders to commit suicide when they are "doxed," or "outed" to their families and the wider public on Ashley Madison (Lucas 2017).

Cyberattacks, both state-sponsored hacktivism and effect-based attacks (Stuxnet), can inflict as much damage as conventional attacks without resorting to force, destruction and killing. Cyberattacks can render communication, transportation, and security systems inoperable leaving a hostile state in a state of disarray, evoking concessions from the government. This points towards the consideration of cyberattacks as an effective tool of pressuring hostile states to concede; thus, potentially reducing tensions. Such outcome would be an ideal case scenario, as the effectiveness of cyberattacks is still a debatable topic. However, treating cyberattacks as purely non-violent alternatives to war would be wrong.

> State-sponsored conflict is virtual, not physical; nonviolent, rather than destructive and malevolent in other respects, equally capable of causing massive social upheaval, or bringing about a “death by 1000 cuts” through pilfering of industrial and state secrets, or by interference in trade, commerce, finance, medical care, and transportation (Lucas 2017).

Cyberattacks are capable of causing death both as direct and indirect result of the attack or hack. Their consideration as non-violent alternatives to war provides only one perspective towards understanding and classifying cyberattacks. Therefore, I consider cyberattacks not only as non-violent alternatives to war, but as violent alternatives to war and acts of war. This offers an opportunity to form the following hypothesis:

- Non-violent alternatives to war should effectively reduce tensions and evoke concessions from the hostile state.

Violent alternatives to war and Acts of war

The discussion of violent alternatives to war starts with several conditions. These conditions cover several understandings about what war is and what constitutes an act of war. Dill (2016, 289, 292) states that “in the twenty-first century war is irredeemable illegitimate” and that “the scale of violence is related to the possibility of controlling and delimiting its effects.” The reason for the irredeemability of war is that “the principles [like IHL or just war theory] [scholars] rely on to guide and assess the conduct of war, both moral and legal, do not even strive to give the individual her moral or (peacetime) legal due” (Dill 2016, 294). I start with these assumptions as under the considerations of irredeemability of war and the aspect of scale, which is not a fixed threshold, clearly delineates violent alternatives of war from the acts of war. Hence, all violent acts can be both considered as acts of war and violent alternatives to war. Furthermore, both violent alternatives to war and acts of war are part of the kinetic force. Gross and Meisels (2017) define kinetic force as hard war.

> Hard war is kinetic: bombs, bullets, and missiles; its outcomes are death, injury, and devastation. Hard war is the chief concern of the international law and moral philosophy (Gross and Meisels 2017).

These considerations help delineate economic war from the actual, physical wars. The primary consideration of violent alternatives to war is that it causes death, injury and limited destruction, unlike the war. Therefore, a question arises when do violent alternatives to war become acts of war? To answer this question, I have to clearly state what I consider as violent alternatives to war, and then analyze examples of VAW, like targeted strikes and special operations, and based on the considerations of scale and effect determine when the violent alternative to war becomes an act of war. The reason I proceeded with this analysis rather than the highlighting and discussing features of non-violent alternatives to war is violent alternatives to war can be very similar to acts of war, however, when carefully defined, violent alternatives to war can be easily distinguished from acts of war. Hence, there is a need to separate these two categories to make sure that the classification of cyberattacks will be more accurate.

Violent alternatives to war can be considered as the last resort option before war takes place. VAWs are the last resort because they are the measures when the non-violent alternatives to war are not particularly effective in dealing with the situation and affect the policy of the hostile state. Hence, I define VAWs as *uses of force that is deployed with an intention to change the policy of the hostile state by intentionally using kinetic measures to damage, destroy or kill targeted system(s) or individuals without crossing a threshold of war*. The Tallinn Manual and Dill (2016, 292) refer to the concept of scale and effect as a deciding factor in the determination whether an armed attack constitutes an act of war[3]. In this sense, I will use the concepts of scale and effect to determine the threshold. I will measure the scale of the attack based on the number of damaged targets and the effect I will consider from the perspective of disruption. The reason I am choosing these factors is scholars used the consideration of the number of casualties that occurred on the battlefield in a given period of

[3] Dill (2016) only refers to the scale and not an effect.

time: 1000 per month. This consideration has been criticized as being subjective as there is no objective criteria to choose this specific number (Wolfendale 2017). The consideration of the spread of destruction and disruption as the result of the use of force offers me a better frame of reference for the determination whether the scale of the attack is large or small, and whether it crosses a threshold of war. If the scale of the attack is large, then it has a higher possibility of becoming an act of war then when the attack is small. The consideration of disruption as an indicator of the effect is used as an umbrella term to depict the duration and the spread of the disruption. To better understand this concept, consider the current pandemic. If the spread of the COVID-19 was proven to be a biological weapon, then considering the scale and the effect, this bio attack would be considered as an act of war. The scale in this sense, refers to the world and the effect of the disruption that the pandemic has caused to the lifestyle of millions of people and economy would make the spread of COVID-19 the act of war. Hence, the disruption accurately depicts the effect of the attack and can be used as an indicator of whether an attack constitutes an act of war or VAW. As a case for the consideration, I will take a targeted strike on a hypothetical weapon plant.

Targeted strike is a perfect example of VAW as the scale and the effect of the attack are relatively contained and do not spillover. Targeted strikes, just like smart or targeted sanctions, attack a specific target and try to cause a minimal amount of collateral damage, while destroying an intended target. Consider a hypothetical case of a construction of a weapon plant in a hostile state. There is evidence that the facility being built is a weapons factory. International community has imposed sanctions on the hostile state, which did not work. Launching a full-scale invasion would be a costly endeavor, which would endanger the lives of civilians, as well as deteriorate tensions further. However, there is a necessity to destroy weapons facilities but with controlled destruction. Hence, the choice would fall to aerial strike either by drone or a jet. The scale of the attack is small, as it would affect only a construction site of the weapon plant. The disruption is relatively small, as the bombing of the construction site would affect the livelihoods of the construction workers, which would be considered as justified collateral damage. Thus, this attack would be considered as a violent alternative to war, as the scale and the effect of the attack did not cause major disruption and suffering to the innocent people. Now, consider another hypothetical case, where a targeted strike was carried out on the functioning electrical grid.

The attack on the electrical grid would not be a justified attack. The attack has been carried out on the electrical grid that supplies power to the weapon manufacturing facility. The problem is that the electrical grid supplies electricity not only to the weapons manufacturing facility but to the town nearby. The result of the bombing on the electrical grid is the cascading failure of the systems within the town. Sewage systems, water supply and emergency systems stop working, which causes a mass distress among the population. Since the intended target was the electrical grid, which led to the cascading failure of the systems, the scale of the attack is large, as the failure of the system is a direct result of the attack. Such an act of aggression would be considered as an act of war, as it disrupts the functioning of a town's major infrastructure points. Hence, the level of disruption exceeds the appropriate levels. Appropriate level would be a temporary blackout and disruption of non-critical infrastructure. Based on this I can formulate the following hypotheses regarding the threshold of when VAW becomes a war:

1. If the scale of the attack is small and the spillover effect have been considered, then the attack is a violent alternative to war;
2. If the effect of the attack is a localized, temporary disruption of non-critical infrastructure, then the attack is a violent alternative to war.

In conclusion, the consideration of NVAW and VAW is based on the considerations that both of these measures intend to affect hostile states' policy to change its behavior; however, they do so through different means. NVAW does so by applying economic or diplomatic pressure on its target; thus, forcing a hostile state to yield to the demands posed by an imposing state (soft war). VAW changes the behavior of the hostile state by getting rid of the leverage of the hostile state by destroying it (hard war). The successful NVAW is when it intends and acts upon the intention to isolate damage to a specific target, without causing an excessive amount of suffering to the innocent population. Furthermore, NVAW should be both a signaling and a punishing tool. It signals to the international community that certain states have committed transgressions and should be punished for them.

VAW is very similar to the acts of war. This makes it difficult to differentiate between which measures would be considered as VAWs and which as acts of war. The answer to this question lays within the consideration and exploration of concepts of scale and effect. The scale is responsible for the determination of whether the attack affected an intended target or did it result in a spillover effect. The concept of effect operates on the consideration of the level of disruption. I propose to use this indicator, as it accurately depicts the effect of the attack by focusing on the severity and duration of the disruption. If the level exceeds the appropriate, which is a localized and temporary disruption, then the attack will be considered as an act of war. With these considerations in mind, I will proceed to the classification of cyberattacks within the categories of NVAW, VAW and acts of war.

Chapter 4. Classification

The main reason for the development of classification is to provide a detailed account of cyberattacks and the way cyberattacks currently are used by states. I will classify cyberattacks within three categories of non-violent alternatives to war (NVAW), violent alternatives to war (VAW) and acts of war. The reason for classification of cyberattacks within all of these categories is the versatility of cyberattacks. Cyberattacks can be non-violent alternatives to war as Gross and Meisels (2017), Lucas (2016, 2017) and Maness, Valeriano, and Jensen (2019) argue. Gross and Meisels (2017) and Lucas (2016, 2017) directly argue this by stating that cyberattacks are part of soft war category, as this form of attack does not use kinetic force to coerce governments or non-government actors into compliance[4]. The way Maness, Valeriano and Jensen (2019) treat cyberattacks in their Dyadic Cyber Incident Dataset (DCID) ver. 1.5 points towards a certain argument. The current state of cyberattacks makes cyberattacks non-violent alternative to war, while authors of the dataset do not disregard the possibility of cyberattacks being violent alternative to war or an act of war. Hence, the aim of this chapter is to present a comprehensible classification of cyberattacks under the categories of NVAW, VAW and acts of war. To accomplish this task, I will refer to the DCID as main basis for the consideration of cases and indicators within the categories of NVAW, VAW and act of war. This chapter will proceed in the following manner.

First, I will discuss what makes alternatives to war violent and non-violent and what makes certain acts of aggression act of war. To do this I will refer to the codebook of DCID, that has a detailed outline of the severity scale for cyberattacks. By using the established categories within the dataset, I more accurately can pinpoint the threshold between violent alternatives to war and acts of war. Second, I will outline the dataset itself and present the

[4] Lucas (2016, 2017) does not decline the possibility of cyberattacks becoming violent alternatives to war, but in the cited works, Lucas analyzes cyberattacks focused on the information warfare.

way I used the dataset, i.e. the case selection and categories that I have considered. Finally, I will describe currently existing cyberattacks and hypothetical cases based on the DCID severity scale, and classify them under the NVAW, VAW and act of war categories.

The difference between non-violent and violent alternatives to war is clear. Non-violent alternatives to war do not use kinetic force to coerce hostile governments into changing their policies. Non-violent alternatives to war do not intentionally cause deaths. Measures, like sanctions, embargoes, and criticism diplomacy are used as an alternative to war. The consideration of deaths is not included within the consideration of their deployment. If deaths occur, they occur not as a direct result of the imposition of sanctions, but from the way governmental and non-governmental actors mitigate the sanctions imposed upon them. Violent alternatives to war coerce hostile governmental and non-governmental actors using kinetic force that end up in deaths. The aspect of harm and deaths to the civilian population is included within the calculation of deployment of violent alternatives to war. Consider a targeted strike or special operation into the enemy territory. These types of measures use kinetic force in the form of boots on the ground, bullets, and rockets, which in one way or another result in deaths of either military and governmental personnel or collateral casualties among innocent civilian populations. The aspect of death is included within the calculation of the deployment and intended to minimize collateral damages. However, the difference between violent alternatives to war and act of war is not so clear.

The difference between the violent alternatives to war and acts of war depends on the consideration of scale and effect of the measure. The Tallinn Manual and Dill (2016, 292) refer to the concept of scale and effect as a deciding factor in the determination whether an armed attack constitutes an act of war. The scientific consideration of the scale and effect is usually measured in terms of deaths on the battlefield over a period of time: 1000 deaths per month. This is not a very useful measurement, as it considers a battle between warring sides and disregards terrorist acts that can be *casus belli*. A much more appropriate measurement of scale and effect would be “severity scale” from the Dyadic Cyber Incident Dataset (Maness, Valeriano, and Jensen 2019, 7–9). The severity scale determines how severe the scale and the effect of a cyberattack is. The scale is graded on the 0-10 scale level, where 0 corresponds to absence of cyber activity, and 10 corresponds to “massive death as a direct result of cyber incident” (Maness, Valeriano, and Jensen 2019, 4 and 7–8). The severity scale provides an accurate and detailed account for different cases of cyberattacks.

Table 2. Severity Scale (Maness, Valeriano, and Jensen 2019, 7–9)

Level	Name	Definition	Examples
0	No cyber activity	-	-
1	Probing/packet sniffing without kinetic cyber	Using cyber methods to breach networks but not utilize any malicious actions beyond that. Hacking a power grid but not shutting it down, planting surveillance technology within networks, and unsophisticated probing methods are examples of this severity level	U.S. NSA dormant infiltrations, packet sniffing
2	Harassment, propaganda, nuisance disruption	Mainly vandalism or DDoS campaigns, this measure is coded when pockets of government or private networks are disrupted for periods of time and normal day to day online life is difficult but recoverable	Propagandist messages in Ukraine, Vandalism, DDoS in Georgia, Bronze Soldier dispute

3	Stealing targeted critical information	This involves the use of intruding upon a secure network and stealing sensitive or secret information. The theft of Lockheed Martin's F-35 jet plans or the U.S. Department of Defense's strategy in the Far East are examples. Or if the target was critical to national security or the objective of the attack had national security implications. The piggy-back method is another example of this severity type. The U.S.' NSA was able to piggy-back on China's Byzantine Series undetected and spy on the targets that the original espionage was spying upon	Chinese targeted espionage, government-sanctioned cybercrime, Sony Hack
4	Widespread government, economic, military, or critical private sector network intrusion	Phishing and intrusion espionage campaigns that successfully steal large troves of critical information, such as the OPM hack	US OPN hack, DoD employee records stolen, IRS hack
5	Single critical network infiltration and physical attempted destruction	This measure entails successful breach of a network where damage is done, however the breached network is left intact in term	Stuxnet, Flame, DoD secure network intrusion

		of functionality and recoverable losses	
6	Single critical network infiltration and widespread destruction	A single network that is critical to national security must be breached and widespread destruction must be successful. Critical stored information is destroyed or unrecoverable or functionality of the network must be limited to non-existent for a period of time	Shamoon, DoD taken offline, Lockheed Martin database wiped out
7	Minimal death as direct result of cyber incident	A state-sponsored cyber incident would be responsible for the death of an individual or group of individuals of another state by either hacking into the automobile of the victim(s) or causing it to crash, or if the victim(s) are dependent on a pacemaker to live and this device is hacked, leading to that person's death	Auto-hacked, pacemaker hacked
8	Critical national economic disruption as a result of cyber incident	A sophisticated infiltration must be responsible for the manipulation of prices that affect stock market indexes and prices for extended periods of time. Another example would be a cyber	Stock market price manipulation, critical e-commerce shut down for extended periods

		incident being responsible for the slowing or shutting down commerce online. This attack must be severe and critically threatening beyond compromising payment systems	
9	Critical national infrastructure destruction as a result of cyber incident	A state's critical infrastructure must be breached, and the network manipulated so that widespread functionality is disrupted for a significant period of time. These efforts have to be massive, impactful, and clearly intentional	Power grid hack, hydroelectric dams shut down, indirect death
10	Massive death as a direct result of cyber incident	A state must direct a cyber incident against another state's or private organizations' network where the system is manipulated, and massive loss of life is a result (over 100 deaths).	NORAD hacked and missiles launched, Air traffic control systems manipulated, commercial airliner hacked and brought down

Provided severity scale provides a clear delineation between all three uses of force. Based on the severity level, I can accurately establish thresholds between NVAW, VAW and acts of war. I propose that the threshold for the NVAW should be at severity level 5 – 6, VAW – 7-8, and acts of war should be set at severity levels 9-10. I consider cyberattacks that fall under levels 0-3 as cyber espionage, as these cases do not fit within the considerations of

NVAW. Cyber espionage affects systems to steal information, to plant backdoors for future intrusions or to spy on an individual or group of individuals. Acts of cyber espionage are not part of the alternatives to war, as they are not part of war effort. Acts of cyber espionage are part of rivalry between states, which happens outside of militarized conflicts. The act of espionage is not an act of war, as the purpose of spying is stealing sensitive information from secure places. Act of war is a use of force that meets the condition of 3Ds: disruption, destruction, and deaths. Destruction of civilian infrastructure that provides basic human needs, like electricity and water, has to be widespread. Disruption of access to basic human needs to the civilian population. Deaths among the civilian population that is the direct result of the use of force. This definition is based on the consideration of multiple arguments and definitions of war and use of force from Gross and Meisels (2017), Maness, Valeriano, and Jensen (2019), Schmitt (2017), and Wolfendale (2017). Since cyber espionage has not resulted in any of the 3Ds, this form of use of force is not an act of war or violent alternative to war. It is its own standalone category.

I set the threshold for NVAW, VAW and acts of war within the severity scale based on the consideration of definitions of alternatives to war and act of war, as well as the nature of current cyberattacks and functions that those attacks serve. Cyberattacks that try to damage isolated systems without affecting civilian infrastructures or causing casualties among civilian population (level 4-6). These attacks do not use kinetic force and do not cause death. This is further supported by the fact that the main cases were chosen cyberattacks that focused specifically on the manipulation of systems to the point of destruction of the non-critical system and temporary malfunction, i.e. Stuxnet and Shamoon. Stuxnet affected a very isolated nuclear facility in Natanz, Iran and caused a malfunction in centrifuges that were enriching uranium, which caused it to break without causing a radiation leak. This operation affected Iran’s nuclear program, which was supposed to halt the development of nuclear weapons, which could be used against Iran's rivals. The attack had accomplished its goal by destroying centrifuges and halting Iran's nuclear program, however, the attack did not use kinetic force to cause a malfunction, neither it resulted in deaths of civilians or disruptions that prevented civilians from accessing basic human needs. This attack was launched to change Iran's behavior; hence, considering the factors these types of attack that attack and disrupt or destruct systems without causing mass disruptions or deaths are classified as non-violent alternatives to war. Furthermore, another set of cases that would be considered as NVAW are level 4 attacks. I refer to some cyberattacks as "hack and dump" cyberattacks. These resemble the criticism of diplomacy or "naming and shaming." The appropriate case for the consideration would be the hacking of Hilary Clinton's emails and then dumping the information to the public. Hackers "named" Clinton's deeds for public "shaming," which negatively affected her reputation and the subsequent standing in the Presidential race.

Violent alternatives to war are cases that correspond to levels 7 and 8 – Minimal death and disruption of economy as a result of a cyber incident (Maness, Valeriano, and Jensen 2019, 8). Conventionally, VAWs are uses of kinetic force that result in localized destruction, disruption, or death. In the cases of levels 7 and 8, deaths are kept to minimal, and the affected system does not disrupt access to basic human needs, as the government would still provide them. I consider these types of cyberattacks as VAWs not because of the kinetic aspect but based on the consideration of direct deaths from cyberattack. Furthermore, cyberattacks that correspond to level 8 are VAWs because of the severity of the attack. The attack affects a system that provides basic human needs to the civilian population and shutting it down or causing a malfunction within it would create a disruption for the civilians. Nevertheless, as the definition of the attack points out – the attack "must be severe and critically threatening beyond compromising payment systems" (Maness, Valeriano, and Jensen 2019, 8). The key characteristic here is the attack must be critically threatening, rather than be a direct cause of a complete failure of critical infrastructure. Cyberattack can be a cause of disruption without causing mass suffering to the civilian population. Hence, these cyberattacks are violent, since they cause deaths and temporary yet severe disruption, but those effects are localized to a specific person (in case of death) or temporary (in case of disruption).

Cyberattacks should be considered as acts of war, if their severity level is 9 and/or 10. I consider as acts of war uses of force that meet the condition of 3Ds – disruption, destruction, and deaths. The uses of force that are direct causes of an extended or permanent disruption of access to basic human needs, widespread destruction of critical infrastructure that gives an access to basic human needs, and massive deaths among civilian populations are acts of war. Levels 9 and 10 depict these characteristics. Level 9 cyberattacks target the state's critical infrastructure to breach it, and the network must be manipulated so that widespread functionality is disrupted for a significant period of time. Cyberattack has to be "massive, impactful, and clearly intentional" (Maness, Valeriano, and Jensen 2019, 8). Imagine a cyberattack that targets a power grid. It can be argued that the power grid is a dual-use system that services both military and civilian sites. Under the Rule 101 of the Tallinn Manual status of military and civilian objectives cannot exist at the same time within the same object, it has to be either one of those (Schmitt 2017, 445). Under this rule all dual-use objects and facilities are military objectives, but to which applies the rule of proportionality. Since, power grid hack is affecting power systems that service civilian facilities, the effects of the attack should not be significant disruption and destruction of infrastructure, as it will indirectly lead to deaths amongst civilian population by denying access to the basic human needs. The denial happens because electricity is needed to keep the hospitals running and ensure that the emergency response teams are working properly. If the hack succeeds in the massive and widespread destruction and disruption, then the hack is an act of war that undermined security of the state and caused deaths of innocent people.

Level 10 cyberattacks are the direct cause of massive deaths. Being a direct cause of massive amounts of death makes a cyberattack an act of war. A point of interest within the definition of this level is the use of word massive and the subsequent provision of the amount of deaths. Maness, Valeriano, and Jensen (2019, 8) specify that the "massive loss of life" amounts to over 100 deaths. This begs a question of the basis for the consideration of this number. The consideration of this number was probably done for the sake of proper codification. Wolfendale (2017) argues that the provision of the fixed number within the definition of war is subjective, as there are no objective criteria for choosing a specific number. However, this does not devalue the definition of the level 10. To overcome this criticism, I will not consider level 10 as a standalone criterion of massive loss of life. I will treat severity levels as a process of accumulation of effects of cyberattacks. For instance, level 10 will entail not only the massive deaths, but also include the characteristics of level 9. Specifically, the aspect of disruption for a significant period of time. This way I will be able to use level 10 without referring to the number of casualties. Therefore, the classification model looks in the following manner.

Table 3. Classification model of cyberattacks

Level	Name	Type of cyberattack
0	No cyber activity	-
1	Probing/packet sniffing without kinetic cyber	Cyber espionage
2	Harassment, propaganda, nuisance disruption	
3	Stealing targeted critical information	
4	Widespread government, economic, military, or critical private sector network intrusion	Non-violent alternatives to war
5	Single critical network infiltration and physical attempted destruction	
6	Single critical network infiltration and widespread destruction	
7	Minimal death as direct result of cyber incident	Violent alternatives to war
8	Critical national economic disruption as a result of cyber incident	
9	Critical national infrastructure destruction as a result of cyber incident	Acts of war
10	Massive death as a direct result of cyber incident	

With the classification being established, I will now present the selection of cases.

For the selection of cases I will use the DCID database, which has extensive information regarding 266 rival dyadic cyberattacks in the period between 2001 and 2016. I have narrowed down the selection of cases from 266 to 9 cases. I have started by eliminating cases based on the interaction between targets and the severity of cyberattacks. During the first round of eliminations, I have chosen cases in which types of interactions are defensive and offensive. I consider only these types of interactions, as defensive operations and offensive strikes are the ones that have a chance to become an act of war and be considered as alternatives to war. Cyberattacks that are classified as nuisance would create a temporary inconvenience to the target state, but it would not be enough to initiate a change within their policies. Defensive or offensive operations would affect policies of the target state, as they are launched to coerce targeted states to change policies by causing malfunction or destroying the system. Next step was to select severity levels. Since, I consider levels 1-3 as cyber espionage, which are not considered as alternatives to war or acts of war, I have omitted them from cases. Hence, I have to consider cases that correspond to levels 4-10; however, this is not the case. Dyadic Cyber Incident Dataset does not contain cases that correspond to severity levels 7 to 10. This means that within the database there are no cases of cyberattacks that could be considered as violent alternatives to war or acts of war. Hence, the severity levels that I will be considering for my case selection is levels 4-6, which correspond to NVAWs. This means that within my case study section, I will provide an actual case of cyberattack for the analysis; however, for the categories of VAWs and acts of war, I will consider cases that were depicted in the popular media (movies and TV series). The last factor I filtered to narrow down cases is the "concession" (Maness, Valeriano, and Jensen 2019, 4). Concession refers to evocation of change in behavior of the target state. It is a binary indicator, which is coded as "0" and "1". Since, the main purpose of alternatives to war is to change the behavior of the target state, I filtered the concession indicator to be positive for evocation of a concessionary change. Hence, my case studies section looks at cases that evoked concessions from the target government, where the government military and non-military facilities were targeted with a severity levels ranging from 4 to 6. Based on the filtering, I was able to narrow down cases from 266 to 9 cases. Out of which I decided to cover the "Stuxnet" as a representative case for NVAWs. For VAWs I will consider a hypothetical case derived from the episode of TV series "Homeland." As for cases of cyberattacks that correspond to acts of war, I choose a hypothetical case derived from the plot of the action movie "Die Hard 4.0."

Chapter 5. Case Studies

The case study section of this thesis consists of analysis of three different cases of cyberattacks actual and hypothetical. Actual case for the consideration is representative of non-violent alternative to war, where criteria for case selection process was that cyberattack evoked concessions from the target government, where the government military and non-military facilities were targeted with a severity levels ranging from 4 to 6. The hypothetical cases were derived from the plots of TV series and movies that depict certain types of cyberattack based on the definitions of violent alternatives to war and acts of war, as well as the definitions of the corresponding severity levels depicted in the previous chapter. The plot of tenth episode of the second season of TV series "Homeland," which depicts the process of hacking of a pacemaker and killing of the Vice-President through the pacemaker. This is a hypothetical representation of a violent alternative to war, as the depicted hack corresponds to the level 7 of the DCID severity scale. The plot of 2007 action movie starring Bruce Willis "Live Free or Die Hard" or "Die Hard 4.0," where depicted a massive cyberattack which can be classified as level 9 and 10 of the DCID severity scale. This hypothetical case is chosen as a representative case of act of war.

This chapter will proceed in the following manner. Each case will be divided into two sections. Within the first section, I will present a detailed presentation of the background of cases – before and during the execution of the attack for Stuxnet, and the plot summary for the hypothetical cases depicted in the popular media. Then based on the consideration of the scale and the effect of the attack, I will present in what aspects does the attack fits within the consideration of alternatives to war and act of war.

Stuxnet

Stuxnet was detected in 2010 as it caused a malfunction within centrifuges that were responsible for the enrichment of uranium at Natanz nuclear facility. The aim of the attack was to disable or halt Iran's nuclear program. Iran potentially acquiring WMDs has been a problem on the international arena since 2006, which is the narrow context that directly leads to the Stuxnet attack. The diplomatic efforts were undertaken by the UN Security Council, as "Resolution 1737 included an embargo of all trade with Iran that encompassed any products or services involved nuclear and ballistic missile programs, a ban on the export or import from Iran of any arms procurement material, and a travel ban on top-level Iranian officials thought to be associated with the program" (Valeriano and Maness 2015, 150). This resolution was followed by UNSC Resolution 1803 in 2008, which enforced the measures of Resolution 1737 and froze Iran's assets (Valeriano and Maness 2015, 150). These resolutions were made due to International Atomic Energy Agency (IAEA) inability to rule out nuclear weapons program in Iran, which creates a possible threat, which has to be dealt with. The actions taken by the UN are justified, as the threat that Iran's nuclear weapons program posed does not warrant use of force, i.e. intervention or direct strike on the facility. It is not imminent and there was no direct evidence of the nuclear weapons program's existence. However, the diplomatic efforts did not work, as Iran did not stop nuclear facility in Natanz, but have increased their output. Hence, the required action here would be one that does not use kinetic force and cause a complete destruction, which could potentially cause a nuclear fallout. Instead, a non-violent action is required, but with diplomacy and sanctions not yielding results, cyberattack is a reasonable action. Determination of whether this case fits within the characteristics of the NVAWs depends on the consideration of hypotheses:

H1: NVAWs should have intention and act upon the intention to isolate damage to a specific target.

H2: The deployed NVAW should shed light on the transgression of the hostile state.

H3: NVAW should ideally effectively reduce tensions and result in concessions of the hostile state.

Regarding the first hypothesis, the Stuxnet attack had an intention to “cripple, destroy, or delay Iran’s nuclear production facilities in order to forestall the need for a conventional attack” (Valeriano and Maness 2015). Furthermore, Valeriano and Maness (2015) argue that “the perpetrator had to develop a timed and precise set of computer code for an old industrial controller, overcome an air gap, make it appear as if the centrifuges were running as normal, and have the bug report back to the controller, all without direct access.” Since, the intent of the cyberattack was to cripple and destroy and served as a “peaceful alternative to direct conventional attack,” Stuxnet was designed to be a precise tool that would tackle a specific exploit in the centrifuges that would cause a malfunction without severe damages (Valeriano and Maness 2015). Designers of Stuxnet had the intention to isolate damage to a specific target without causing a spillover effect. They acted upon it, as the Stuxnet was designed to be directly plugged into the computer that controls centrifuges and launched there. It eventually caused a malfunction in the centrifuges, which did not cause a severe damage to the nuclear facility; hence, supporting the hypothesis #1, which states that NVAW should have intention and act upon that intention to isolate effects of damages as much as possible.

Regarding the second and third hypotheses, Stuxnet does not firmly support them for several reasons. Hypothesis #2 states that NVAW should shed light on transgressions, which is true for the initial launched NVAW. In the case of Iran’s nuclear program, the initial NVAW was not Stuxnet attack. The initial NVAW were sanctions that were imposed under Resolutions 1737 and 1803 (Valeriano and Maness 2015). These sanctions were the initial NVAW, which successfully shed light onto Iran’s development of nuclear weapons. Hence, the Stuxnet attack does not satisfy the hypotheses #2, as the international community has already known that Iran was engaged in the alleged development of nuclear weapons.

Regarding the hypothesis #3, which refers to the effective reduction of tensions and evocation of concessions of the hostile state, Stuxnet did evoke concessions from Iran in the form of a much more defensive stance from Iranian government rather than halting their nuclear program, as the halting of nuclear program would not be fully discussed until 2015. Furthermore, Valeriano and Maness (2015) argue that the impact that Stuxnet had on the progression of Iran's nuclear program is debatable, as Barzashka (2013), Lindsay (2013) and multiple other scholars have different perspectives on the effectiveness of Stuxnet attack. For instance, Lindsay (2013) argues that Stuxnet only temporarily halted the production rate of enriched uranium at Natanz. Hence, Stuxnet does not fully satisfy the third hypothesis. However, this does not cross out Stuxnet from being a NVAW. The third hypothesis relates to an ideal case scenario, where deployed NVAW results in tensions reduction and subsequent concession of the target state. At the end, Stuxnet is a peaceful alternative to war that was deployed as a last resort option, when sanctions did not yield positive results. The cyberattack was designed with an intention to cause a malfunction within a system, which corresponds to the level 5 severity, without causing harm to innocent civilians in the form of deaths or significant disruption of access to the basic human needs. Hence, based on these considerations, Stuxnet is a representative case of a non-violent alternative to war, as it did not use kinetic force to casualties among the civilian population.

Pacemaker hack

The case of Pacemaker Hack refers to the case depicted in the tenth episode of the second season of TV series "Homeland." This particular episode contains a scene, where a terrorist hacker, breaches into the U.S. Vice-President's pacemaker and causes an intense heart fibrillation and causes a heart attack, which kills the Vice-President. The question arises of whether such an attack is possible. The answer is yes.

> While the whole operation seemed almost too simple, it's not a completely implausible tactic. In October of [2012] Darren Pauli wrote at *SC Magazine* that a researcher in Australia "reverse-engineered a pacemaker transmitter to make it possible to deliver deadly electric shocks to pacemakers within 30 feet and rewrite their firmware" (Zuckerman 2012).

Such execution of a targeted attack is a terrorist act, as the episode depicts a terrorist killing the VP of the U.S. for its malicious goals. Such attack would not be considered as a violent alternative to war, but as act of terrorism and murder. However, since there are no real-life cases of such attacks happening, this scenario is hypothetical, which I can modify. Consider that instead of a terrorist performing a hack but a government-sponsored hacker and the target is not VP of the U.S. but a terrorist or a key member of the hostile government, who is directly responsible for the atrocities that happen within the territory of a hostile state. Then, the attack can be considered through the characteristics of violent alternatives to war.

Determination of the Pacemaker Hack as a violent alternative to war depends on the consideration of two hypotheses. The first hypothesis states that for the attack to be considered as a violent alternative to war, the scale of the attack must be small, and the spillover effect should be included within the calculations of the attack. The Pacemaker Hack corresponds to the level 7 of the DCID severity scale – Minimal death as direct result of cyber incident. It is a very localized attack that is contained to a single target without spilling over to the public sector and causing mass deaths among the civilian population. The attack fits within the definition of violent alternative to war – a kinetic use of force that is deployed with an intention to change the policy of the hostile state by causing damage to the targeted system(s) without crossing a threshold of war. Hence, the Pacemaker Hack supports the first hypothesis.

Pacemaker Hack also supports the second hypothesis. The second hypothesis refers to the effect of the attack being localized with temporary disruption of non-critical infrastructure. The government official responsible for policies of the state is critical infrastructure; however, the disruption that the Pacemaker Hack did is temporary, as instead of the deceased official, the head of the government would appoint another person, which could potentially reduce tensions and result in concessions of the hostile government. Nonetheless, the pacemaker hack by affecting a single person makes the effect of the attack to be localized and contained, which creates a temporary disruption within the government. Therefore, by supporting both hypotheses, Pacemaker Hack classifies as a violent alternative to war, as the created damage does not cross the threshold of war, which is satisfaction of the rule of the 3Ds.

Die Hard 4.0

The case of Die Hard 4.0 refers to a massive cyberattack that is classified as an act of war. According to the plot, a terrorist group conducts a series of cyberattacks in three stages, which is called “Firesale.” During stage one, a group hacks the FBI Cyber-security division, which is followed by an attack on the Traffic control center and taking complete control over their systems, causing mass accidents on the streets of Washington DC. The attack on the Traffic control center is followed by a cascade failure of the critical infrastructure of the U.S., such as Aviation control, L-train network in Chicago, and breaching into the Department of Homeland Security network. During the stage two of the attack, the group attacks the Wall Street manipulating stock prices. Stage three is responsible for shutting down all the utilities in the country. The result of the cyberattack on the transportation system is the massive collapse and subsequent casualties due to mass traffic accidents. The severity of these attacks corresponds to levels 9 and 10 of the DCID severity scale – destruction of critical national infrastructure and massive deaths as a direct result of the attack. These severity levels are representative of the acts of war. However, to be confident in the correct classification, I will consider the plot of Die Hard 4.0 in the context of definition of acts of war.

The series of cyberattacks depicted in Die Hard 4.0 fit within the rule of the 3Ds. The rule of the 3Ds provides conditions that need to be met for an attack to be considered as an act of war. The rule consists of destruction, disruption and deaths. The use of force has to cause a widespread destruction of systems and/or infrastructure that causes a significant disruption of access to the basic human needs for civilians, and cause mass deaths of innocent civilians. The Firesale attack conducted by a terrorist group causes a widespread destruction, as the critical infrastructure is breached and is shut down. This is further followed by a significant disruption, as the emergency services are overwhelmed by a barrage of affected people and cannot respond to them in a timely manner. As a result of the cyberattack, there are casualties among the civilian population, which are directly and indirectly caused by the Firesale attack. The thing about this attack is that it would be classified as a terrorist act, which was initiated by a domestic terrorist group; however, if such an attack happened because of the international terrorist group or the foreign government, then the attack would be considered as an act of war. Launching cyberattack on such scale would be unjust, as there is an intent to damage critical infrastructure that is used by the civilians and disrupts their lives, making them a target of the attack.

Chapter 6. Conclusion

Within my thesis I attempted to answer the question of cyberattack classification as non-violent alternatives to war, violent alternatives to war, and acts of war. I argue that cyberattacks should not be limited to the category of non-violent alternatives to war and should also be considered as violent alternatives to war and act of war. To accomplish this task, I needed to establish several core definitions. By establishing these core definitions, I will be able more accurately classify existing and hypothetical cases of cyberattacks.

First core concept is concerned with the constitution of the act of war. Wolfendale (2017) provides definitions of war derived from various fields. Wolfendale (2017) presents definitions of war from the perspectives of just war, jurisprudence, political science, and sociology. These definitions serve specific purposes, which make them very limited in their application. Most of the limitations come from the consideration of war as a phenomenon of morality, law, intent, and statistics, which explain certain behavioral patterns of war but do not state specifically what constitutes an act of war. Wolfendale (2017) criticized in detail the sociological definition of cyberattacks. The sociological definition of cyberattacks provides a specified number of casualties for a battle to be considered as an act of war. The use of a specific number of casualties makes the difference between "war and lesser conflicts" arbitrary. I agree with her critique, as the consideration of specific number of casualties on the battlefield does not take into consideration the possible suffering of civilians. The consideration of effect can provide an explanation for "when and why a conflict becomes a war," which include the aspect of disruption of access to basic human needs for civilian population (Wolfendale 2017). The disruption itself happens when certain critical infrastructure is damaged or destroyed, and the disruption itself leads to the deaths of the civilian population. Hence, for an attack or a use of force to be considered as an act of war, I propose the rule of the 3Ds. The use of force is an act of war when it meets the criteria of 3Ds:

4. Act of war should cause mass destruction of property.
5. Act of war should cause a significant disruption of provision of basic human needs.
6. Act of war should cause massive deaths among the civilian population or members of the military.

Hence, the definition of the act of war is the use of force that causes widespread destruction, significant disruption of basic human needs and cause of massive deaths (direct and indirect).

Second and third core concepts are concerned with the non-violent and violent alternatives to war. These concepts are derived from the concepts of Gross and Meisels (2017) soft and hard wars. Soft war encompasses measures that are non-violent, i.e. non-kinetic. Hard war encompasses measures that are violent, i.e. kinetic.

> Soft war is non-kinetic war. Bytes, boycotts, propaganda, nonviolent resistance, and even kidnapping replace bullets and bombs and supplant the predominant role of lethal force that captures or images of war. Unarmed force is not deadly but it also not passive. It may be soft to the touch but is as coercive as any act of terrorism or targeted killing. <…> Hard war is kinetic: bombs, bullets, and missiles; its outcomes are death, injury, and devastation. Hard war is the chief concern of the international law and moral philosophy (Gross and Meisels 2017).

Soft war compared to hard war is conducted without using bullets but with applying political and economic pressure, which evokes concessional changes in hostile states. Soft war measures do not use kinetic force to force states, as the state using soft measures applies pressure to certain sectors without causing deaths, like the hard war measures, which include the consideration of deaths within the process of deployment justification. The applied pressure comes from the economic limitations or ban on selling and buying arms, as well as application of diplomatic pressure through the deterioration of diplomatic relations. Gross and Meisels (2017) consider economic sanctions, arms embargoes, diplomatic criticism, and cyberattacks as measures of soft war.

“Cyber conflict of one type should be included within the purview of “soft” or “unrestricted” warfare,” which is “state-sponsored hacktivism” (Lucas 2017). Cyberattacks and especially state-sponsored hacktivism have not caused any casualties among the civilian population. Cyberattacks have been the cause of defacement of websites and the crash of governmental facilities, but the damage was not enough to cause severe injuries to civilians’ bodies or minds. Hypothetically, there could be a cyberattack that will disable the electric grid or damage the nuclear reactor to the point of meltdown or the situation where the hacking of a control tower results in a crash of several planes; however, these all are hypothetical cases, which were not reproduced in the real world. Hence, since cyberattacks have not caused kinetic harm, they are considered as non-violent alternatives to war seems to be more suitable; however, adopting the position that cyberattacks are non-violent alternatives to war only completely ignores the fact that cyberattacks are also violent alternatives to war.

After this, I have established a theoretical framework, where I discussed what makes sanctions, embargoes, diplomatic criticism, targeted strikes non-violent, violent alternatives to war and acts of war. The consideration of the nature of these measures of the use of force have led me to the following conclusions. Based on the consideration of economic sanctions, arms embargoes, and diplomatic criticism, non-violent alternatives to war should

- Have an intention and act upon it to isolate the damage to a specific target.
- Shed light to the international community on the transgressions that certain states have performed.
- Effectively reduce tensions and evoke concessions from the hostile state.

These criteria are based on the considerations that non-violent alternatives to war should not intentionally cause death or significant suffering among the civilian population. The effect of sanctions, arms embargoes, and diplomatic measures should be limited to specific individuals, who are responsible for the transgressions of the hostile state. Also, non-violent alternatives to war should draw the attention of the international community to the transgressions of the hostile state. This means that besides punishing hostile states and pressuring them to concede, non-violent alternatives to war should signal to the international community that the hostile state is committing atrocities or violating international laws. The last condition can be applied in the ideal case scenario, where non-violent alternatives to war result in concessions and change in behavior.

The nature of violent alternatives to war makes them look similar to the acts of war. All violent acts can be both considered as acts of war and violent alternatives to war. Both violent alternatives to war and acts of war are part of the kinetic force. Conceptually, they are different, as violent alternatives to war are uses of force that is deployed with an intention to change the policy of the hostile state by intentionally using kinetic measures to damage, destroy or kill targeted system(s) or individuals without crossing a threshold of war. Hence, there should be a delineating variable that would separate two notions from one another. The aspects of scale and effect, which are not a fixed threshold, clearly delineates violent alternatives of war from the acts of war. For scale and effect, I chose the spread of destruction and disruption based on the consideration of the number and type of affected infrastructure and how widespread and how long was the disruption of access to basic human needs. Based on this, I proposed the following hypotheses for violent alternatives to war:

- If the scale of the attack is small and the spillover effect has been considered, then the attack is a violent alternative to war.

- If the effect of the attack is a localized, temporary disruption of non-critical infrastructure, then the attack is a violent alternative to war.

To test these hypotheses, I referred to the Dyadic Cyber Incident Dataset (DCID) that includes the severity scale. The severity scale determines how severe the scale and the effect of a cyberattack is. The scale is graded on the 0-10 scale level, where 0 corresponds to absence of cyber activity, and 10 corresponds to "massive death as a direct result of cyber incident" (Maness, Valeriano, and Jensen 2019, 4 and 7–8). The severity scale provides an accurate and detailed account for different cases of cyberattacks. Under the considerations of the severity scale, I have classified non-violent alternatives to war on level 4-6. Cyberattacks that try to damage isolated systems without affecting civilian infrastructures or causing casualties among civilian population (level 4-6). These attacks do not use kinetic force and do not cause death. This is further supported by the fact that the main cases were chosen cyberattacks that focused specifically on the manipulation of systems to the point of destruction of the non-critical system and temporary malfunction, i.e. Stuxnet and Shamoon. Violent alternatives to war on level 7-8. VAWs are uses of kinetic force that result in localized destruction, disruption, or death. In the cases of levels 7 and 8, deaths are kept to minimal, and the affected system does not disrupt access to basic human needs, as the government would still provide them. I consider these types of cyberattacks as VAWs not because of the kinetic aspect but based on the consideration of direct deaths from cyberattack. Furthermore, cyberattacks that correspond to level 8 are VAWs because of the severity of the attack. The attack affects a system that provides basic human needs to the civilian population and shutting it down or causing a malfunction within it would create a disruption for the civilians. Acts of war correspond to levels 9-10. Level 9 cyberattacks target the state's critical infrastructure to breach it, and the network must be manipulated so that widespread functionality is disrupted for a significant period of time. Cyberattack has to be "massive, impactful, and clearly intentional" (Maness, Valeriano, and Jensen 2019, 8). Imagine a cyberattack that targets a power grid. It can be argued that the power grid is a dual-use system that services both military and civilian sites. Level 10 cyberattacks are the direct cause of massive deaths. Being a direct cause of massive amounts of death makes a cyberattack an act of war. Levels 1-3 I consider to be representative of cyber espionage, which are not part of war or pre-war effort, as cases of cyber espionage happen outside of conflicts.

To see whether the classification accurately reflects the cases of cyberattacks, I have chosen three cases, where one is an actual case of cyberattack, and the other two are derived from plots of movies and TV shows. The actual case is Stuxnet, which I classify as a non-violent alternative to war. Stuxnet attack had an intention to "cripple, destroy, or delay Iran's nuclear production facilities in order to forestall the need for a conventional attack" (Valeriano and Maness 2015). Designers of Stuxnet had the intention to isolate damage to a specific target without causing a spillover effect. They acted upon it, as the Stuxnet was designed to be directly plugged into the computer that controls centrifuges and launched there. It eventually caused a malfunction in the centrifuges, which did not cause a severe damage to the nuclear facility.

Next case, I took from the plot of an episode from the "Homeland" TV series and classify it as a violent alternative to war. I call it Pacemaker Hack. The Pacemaker Hack corresponds to the level 7 of the DCID severity scale – Minimal death as direct result of cyber incident. It is a very localized attack that is contained to a single target without spilling over to the public sector and causing mass deaths among the civilian population. The attack fits within the definition of violent alternative to war – a kinetic use of force that is deployed with an intention to change the policy of the hostile state by causing damage to the targeted system(s) without crossing a threshold of war. Furthermore, the government official responsible for policies of the state is critical infrastructure; however, the disruption that the

Pacemaker Hack did is temporary, as instead of the deceased official, the head of the government would appoint another person, which could potentially reduce tensions and result in concessions of the hostile government. Nonetheless, the pacemaker hack by affecting a single person makes the effect of the attack to be localized and contained, which creates a temporary disruption within the government.

The last case is derived from the plot of "Die Hard 4.0," which I classify as an act of war. It depicts a series of cyberattacks called "Firesale", which affect critical national infrastructure and cause deaths of civilians. The series of cyberattacks depicted in Die Hard 4.0 fit within the rule of the 3Ds. The rule of the 3Ds provides conditions that need to be met for an attack to be considered as an act of war. The rule consists of destruction, disruption and deaths. The use of force has to cause a widespread destruction of systems and/or infrastructure that causes a significant disruption of access to the basic human needs for civilians, and cause mass deaths of innocent civilians. The Firesale attack conducted by a terrorist group causes a widespread destruction, as the critical infrastructure is breached and is shut down. This is further followed by a significant disruption, as the emergency services are overwhelmed by a barrage of affected people and cannot respond to them in a timely manner. As a result of the cyberattack, there are casualties among the civilian population, which are directly and indirectly caused by the Firesale attack.

I have accomplished the task of this thesis by providing a classification model that accurately defines and classifies cyberattacks. However, there is a proposal for future research. Since, the rule of the 3Ds is developed within the context of this thesis, it would be fruitful to test this definition through empirical research that would look at various acts of war and see, whether the definition holds up against various forms of acts of war, like invasion or intervention (humanitarian and/or military).

Bibliography

Barzashka, Ivanka. 2013. "Are Cyber-Weapons Effective?" *The RUSI Journal* 158(2): 48–56.

Caron, Jean-François. 2019. *Contemporary Technologies and the Morality of Warfare: The War of the Machines*. 1st edition. London ; New York: Routledge.

Gross, Michael L., and Tamar Meisels, eds. 2017. *Soft War: The Ethics of Unarmed Conflict*. Cambridge: Cambridge University Press. https://www.cambridge.org/core/books/soft-war/E1A1AC1A137D46792396EE55F6A5255D (January 30, 2021).

Jensen, Eric Talbot. 2016. "The Tallinn Manual 2.0: Highlights and Insights." *Georgetown Journal of International Law* 48: 735.

Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22(3): 365–404.

Lucas, George. 2016. *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. 1 edition. New York, NY: Oxford University Press.

———. 2017. "State-Sponsored Hacktivism and the Rise of 'Soft' War." In *Soft War: The Ethics of Unarmed Conflict*, eds. Michael L. Gross and Tamar Meisels. Cambridge: Cambridge University Press, 77–87. https://www.cambridge.org/core/books/soft-war/statesponsored-hacktivism-and-the-rise-of-soft-war/23B778712EF4668AB7EE62B095932D30 (January 30, 2021).

MacFarquhar, Neil. 2017. "Denmark Says 'Key Elements' of Russian Government Hacked Defense Ministry." *The New York Times*. https://www.nytimes.com/2017/04/24/world/europe/russia-denmark-hacking-cyberattack-defense-ministry.html (April 6, 2021).

Maness, Ryan C., Brandon Valeriano, and Benjamin Jensen. 2019. "Codebook for the Dyadic Cyber Incidentand CampaignDataset (DCID) Version 1.5." http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/dcid_1.5_codebook.pdf.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). 1986. (International Court of Justice).

Orend, Brian. 2006. *The Morality of War*. 1 edition. Peterborough, Ont.: Broadview Press.

Pattison, James. 2018. *The Alternatives to War: From Sanctions to Nonviolence*. Oxford, New York: Oxford University Press.

Roscini, Marco. 2014. *Cyber Operations and the Use of Force in International Law*. Oxford, New York: Oxford University Press.

Schmitt, Michael N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2 edition. Cambridge, United Kingdom ; New York, NY, USA: Cambridge University Press.

"Tracking State-Sponsored Cyberattacks Around the World." *Council on Foreign Relations*. https://www.cfr.org/cyber-operations (April 3, 2021).

Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. 1 edition. Oxford ; New York: Oxford University Press.

Wolfendale, Jessica. 2017. "Defining War." In *Soft War: The Ethics of Unarmed Conflict*, eds. Michael L. Gross and Tamar Meisels. Cambridge: Cambridge University Press, 16–32. https://www.cambridge.org/core/books/soft-war/defining-war/E93C966D8C3B63369FD04A53331DDD4E (February 15, 2021).

Zuckerman, Esther. 2012. "Just How Impossible Was Last Night's 'Homeland' Episode?" *The Atlantic*. https://www.theatlantic.com/culture/archive/2012/12/just-how-impossible-was-last-nights-homeland-episode/320910/ (April 1, 2021).