Cyber Conflict in the 21st Century

The Future of War and Security in a Digitalizing World

by

Steffen Westerburger

(3041379)

Master Thesis International Relations

In fulfillment of the requirements for the degree Master of Science in Political Science

Radboud School of Management

Radboud University

December 2014

Supervisor: Prof. Dr. J.A. Verbeek

Co-supervisor: Dr. G.C. van der Kamp-Alons

Acknowledgements

I started to write this thesis in February 2014. I am proud that, after a process of nearly ten months, I have completed this research project with which I hope to successfully conclude my master program in International Relations at Radboud University. It marks the end of six years of academic education; a truly unique and indispensible period in my life.

This thesis would not have been possible without the unwavering support of my supervisor, professor Bertjan Verbeek. Throughout the process of writing this thesis you were always there to assist me and provide me with guidance where needed. You really triggered my scientific imagination. Thank you so much. Also I would like to thank Dr. Gerry van der Kamp-Alons for co-supervising this thesis.

I would also like to thank all the friends I met during my studies at Radboud University. Together we were not only able to study, but also to enjoy all the other benefits of being a student. Together we encouraged each other to get the best out of ourselves.

Finally, I would like to express my deepest gratitude to my family. My parents and sister always told me to follow my heart and to do what I most like. Your steadfast support and our many discussions at the dining table were truly invaluable.

Abstract

In the year 2013, threats originating in cyberspace for the first time in history topped the *Global Threat Assessment* of the United States Director of National Intelligence (DNI), a list naming the most pressing national security challenges to the United States. In recent times, rapid technological developments have created a new domain of international politics. These developments mark the 'birth of cyberspace'. New technologies provide us with unimaginable possibilities, our world becomes more interconnected with the day. However, it also creates a new domain for conflict. Cyber conflict. This thesis's main aim is to come up with an assessment on the future of war and security in this digitalizing world. It seeks to come up with answers by testing two hypotheses in nine different cases. Firstly, the role of non state and hybrid actors in the cyber domain is investigated. Secondly, the specific targets of cyber operations are looked into more in detail. This thesis's conclusion is that the influence of developments in the cyber domain is not to be underestimated. Although it is difficult to give a precise assessment of the future of war and security, it is only a matter of time until cyber operations will become more important. We will never again live in a world without cyber. Cyber is here to stay.

Key words: cyber warfare – nature of war – nature of security – information technology – actors in cyberspace – critical infrastructure

Index

List of Tables

1. Introduction

The most recent *Global Threat Assessment* (2013) issued by the Director of National Intelligence (DNI) of the United States James R. Clapper does not mince words: threats to national security are more diverse, interconnected and viral than at any time in history. The assessment's introduction shows a clear image of 'how quickly and radically the world and our threat environments are changing' and results in the inevitable conclusion that these changes 'are demanding reevaluations of the way we do business' (p.1). The report comes up with a rather surprising threat assessment: although one might expect terrorism, weapons of mass destruction or transnational organized crime to top the list of most dangerous threats to US National Security, neither of them in reality do. For the first time in history cyber threats are at the top of this influential report, which is causing heavy debates in US Congress every year. Cyber threats are described to be the number one type of danger facing the United States. 'As more and more state and non state actors gain cyber expertise, its importance and reach as a global threat cannot be overstated' (*ibid*, p.2), Clapper said.

Recently also security scholars have paid more attention to these increased cyber threats, therewith recognizing that cyberspace has grown into an important and new domain of possible conflict that is likely to – as technology rapidly advances - gain more importance in the future. For example Eriksson and Giacomello (2006, p.221) describe the present situation to be one in which states and societies all over the world are becoming increasingly dependent on information technologies (IT). They point at the build-up of interconnectedness of information and communications technologies (ICT) and are specifically pointing towards its most influential one, the internet. In only a few decades the internet has grown faster than one at first sight could have ever imagined. As a result of these developments, the overall costs of using these advanced communications technologies have dropped in such a way that it has become available to an even bigger number of people across the globe (*ibid.* p.222).

In the 21st century – in order to function well - both state and non state actors are increasingly more dependent on information and information technologies. Lin (in Art 2013, p.476-477) gives several striking examples: businesses rely on information technologies (IT) to conduct their

operations; distribution networks for food, water and energy rely on IT in literally every stage, as do health care, transportation and many more key parts of a national and global economy. Naturally, this dependency on technology also has consequences for security, mainly because of two reasons.

First, also military organizations are becoming more and more reliant on IT. Information technology is used to manage and control military processes such as command and control of weapon systems and logistics. Nowadays it is almost unthinkable to operate a modern army without using advanced information systems and technology. Technological knowledge and expertise is one of the key enablers for conventional military success.

Second, the technological developments in itself have created a potential new domain for conflict: cyberspace. Cyberspace is a new, completely digitalized domain in which IT may be used to 'fight' conflicts using 'computers instead of bombs'. These possibilities of digital conflict may have an effect on contemporary international relations theory.

1.1 Actors in Cyberspace

The unique nature of cyberspace has potentially far-reaching effects. The information revolution has created a security domain of which not only state actors, but also non state actors can more easily be part of due to the relatively low costs (*ibid.* p.477-478). For example terrorist organizations have also proven to be experienced in using IT. Whereas we usually witness generally low-tech and underdeveloped kinetic weapons in terrorist organizations, the IT capabilities of terrorists to train, recruit, communicate and engage in terrorist actions are usually highly advanced. Many authors have stressed the fact that the very nature of information technology is such that a wide range of actors can conduct operations of national-level significance (Lin 2013, Eriksson and Giacomello, 2006). For example Peter Singer (2011) was one of the first to bring up and explore a new industry of privatized military companies providing military services for hire. This new industry heavily profits from IT innovations and the 'birth of cyberspace'. Because of the highly advanced knowledge needed to successfully operate in cyberspace, it more often pays off for states to hire the specialized private companies for improving their ICT to help them achieving their military goals. This could lead to the situation in which states became dependent of private companies for operating their armies; it is not

unthinkable that in the future a state has the physic capabilities (for example drones, missiles), but not the crucial technology needed to operate them. This can have major consequences.

Generally speaking we can distinguish two main categories of importance considering potential actors in cyberspace. Firstly, it is obvious that states are an important actor in cyberspace just as they are in the conventional security domain of conventional warfare. States both have the capacity and the motives to engage in war and conflict in cyberspace in order to ensure their survival and pursue their self-interest. It would be rather logical for states to be fully prepared and equipped to act in cyberspace, given the fact that potential adversaries will act accordingly and states' vital interests in the future can only be secured if a state is also capable of acting in cyberspace. Besides, cyber capabilities could turn out to be relatively cheap and interesting complement to a state's military capabilities. As an example, it is generally believed that the United States together with Israel have conducted an offensive cyber attack when they launched their *Stuxnet* worm against Iranian nuclear infrastructure (Farwell and Rohozinski, 2011). Achieving this same outcome with conventional military means would have been more expensive and difficult (*ibid.).*

Secondly, to a much larger extent as in the conventional security domain we can see a variety of non state and hybrid actors capable of being active in cyberspace. Most notably one could think of individuals, organized crime and terrorist organizations. Acting in cyberspace can be really cheap and accessible, some authors like Lin (2013, p.479) point at the fact that these non state actors might conduct attacks in cyberspace 'with information and software found on the Internet and hardware available at Best Buy or Amazon'.

In contrast to motivations one would generally expect states to have for actions in cyberspace, the motivations of these non state actors are divergent. An important reason for these non state actors to be involved in conflict in cyberspace is financial. As noted earlier as an effect of the IT-revolution more and more businesses and financial infrastructures rely on IT. This makes them attractive target for financially driven attacks. Other motives could be political (sending a political message to a broad public) or personal (a hacker wants to show his experience and performance).

Another considerable motive for non state actor to be active in cyberspace is military in nature. It is likely that as an effect of the relatively accessible nature of cyberspace, non state actors

might wage war to pursue their interests. Reasons for warfare in cyberspace are similar to those of conventional warfare, but the means are different. No tanks or rockets are used, but computers. It is about *bits on the ground* instead of *boots on the ground*.

It is generally believed that in a couple of instances in the recent past, states paid individuals to make them privately attack assets in several countries. For example it is believed that the Russian government paid individuals to engage in a cyber attack against Estonia in 2007 and Georgia in 2008, and that the Chinese government actively recruits individuals for these purposes as well (Goodman, 2010).

1.2 The Nature of War and Security in Cyberspace

Conflict and war in cyberspace have different characteristics than wars in the physical space. For the study of international relations in general and the study of war and peace in specific, it is interesting to investigate the magnitude and effects of these differences. Lin (2013, p.480) states the most important and influential differences between conflict and cyberspace and conflict in physical space.

First, Lin points at the *venue for conflict*, herewith pointing at the great difference in where military activities occur. According to Lin traditional kinetic conflicts (TKC) as mostly seen in physical space have a venue for conflict that is largely separate from the space were the vast majority of civilians (and thus non-combatants) is found. In cyberspace this clear separation is not necessarily in place. The space in which cyber conflict occurs, is a place where civilians are omnipresent. This may lead to a situation in which the distinction between combatants and non combatants disappears. The possible disappearance of this distinction can have consequences on the impact of war and conflict and may affect ideas about what constitutes just or unjust wars in international relations in the future (see Walzer, 2006)

Second, in cyberspace a completely different *offense-defense balance* can be identified. In TKC it is usually the case that offensive and defensive capabilities are in balance. Conflicts in cyberspace critically change this picture. In cyberspace the offense – at least at firstly – is inherently superior to the defense. In order to successfully attack in cyberspace, the offensive act only has to be successful once whereas the defense has be successful time after time.

Third, an important characteristic of war and conflict is the capability to be able to verify who in fact was behind the attack against your interests. In TCK usually this does not cause a lot of problems, since in most cases it is pretty clear who is the adversary[1]. Military forces are usually under the clear guidance of a state's government. In cyberspace this is not necessarily true, a problem of *attribution* arises. It is not always the case that actors clearly are governed by states and due to the venue of conflict it is often difficult to actually see who is attacking you. Attribution of a hostile act to a specific state is therefore problematic.

Fourth, *capabilities* between state and non state actors are more in balance in the domain of cyberspace. In TKC the case is clear-cut. It is almost impossible for non state actors to develop military capabilities that are even close to equal the capabilities of states. In cyberspace this is different, non state actors can more easily produce large-scale effects that before only large-scale actors could produce.

Finally, the importance of national borders of sovereign states and the importance of distance are different in cyberspace. In TKC geographical vicinity and distance are of a great importance in order for traditional warfare to be effective. Distance can be a key deciding factor vis-à-vis a potential adversary. If one state is capable of attacking at a distance the other state is not capable of, this creates an important and probably decisive difference. In cyber conflict these issues are not at play and are rather irrelevant. For a cyber attack to be successful, it does not matter whether or not national boundaries need to be crossed.

Due to these differences in the way war and conflict look like in the conventional domain and in the cyber domain, the interesting question arises whether the nature of war itself has not changed as an effect of developments in the cyber domain. If this indeed is the case, this would require scholars of international relations to reconsider their insights and theories.

Certain scholars in International Relations have already tried to answer this question and published extensively on the changing nature of war through the times (see for example Freedman 2013, Keegan 2004, Van Creveld 2009, 2010, Kaldor 2013, Buzan, Waever & De Wilde, 1998) and its

[1] This is not always the case. A good example is the war in Eastern Ukraine (2013-now), a clear sign that it is not always easy to know who you are fighting against.

effects on the nature of security. Kaldor in her book *New and Old Wars: Organized Violence in a Global Era* makes a distinction between 'new' and 'old wars'. According to her new wars can be contrasted with old wars 'in terms of their goals, the methods of warfare and how they are financed'(Kaldor 2013, p.7).

Although these scholars have published extensively on technological developments and their possible changing effect on the nature of war, in many of their contributions the new domain of cyberspace seems to be largely omitted. This surpassing of cyberspace and its effects on the nature of war and conflict is unfortunate. These days the world is rapidly changing into a world in which conflict and war by and against (non) states is literally a mouse click away. Was former Secretary of Defense of the United States really exaggerating when he publicly warned for the possibility of a 'cyber Pearl Harbor'? Was the anonymous US senior official really joking when he privately spoke about his fear that potential future cyber attack on the United States could 'make 9/11 look like a tea party'? Probably they weren't being funny at all, the very fact that until this moment there have been no devastating attacks, originating in cyberspace, that in fact threatened a state's survival in the international system does not provide us with any guarantees for the future. Changes in cyberspace could have far reaching consequences; for example one could ask what effects the aforementioned cyber developments – most notably the likely situation that non state actors will become increasingly important - will have on a state's legitimate monopoly of violence. Kaldor for examples states that 'the monopoly of violence is eroded from below by privatization.' (p.6). If privatization is capable of doing so, why would cyber not be?

1.3 The Concept of Security

In order to be able to judge whether these differences in characteristics of war between the physical space and cyberspace indeed have far-reaching consequences for a state's security, it is important to have a clear definition of the concept of security and to assess whether in the current cyber age 'conventional' concepts of security are still relevant.

The definition of security has been debated upon for decades with different scholars each stressing different parts of what they think constitutes security. Walter Lipmann (1944) describes

security to be 'the capability of a country to protect its core values, both in terms that a state need not to sacrifice core values in avoiding war and can maintain them by winning a war'. Wolfers (1962) agrees on this, stating that security is the absence of threats to a society's core values. Ullman (1983) puts it more concise, according to him security is 'a decrease in vulnerability'. Buzan (2000) expands the definition of security by stressing that international security is more than the mere study of threats, moreover it is also a study of which threats are to be tolerated and which require immediate action. Consequently, security is something between power and peace.

Fierke (2007, p.4-5) could be seen as one of the leading scholars of the so called critical security studies (CSS) school of thought. Her main argument is that definitions of security are inherently politically and contextually bound. The fact that usually security is being seen in the fixed and narrow military definition (stressing the threat and use of force) is a clear outcome of a specific political and historical environment. She stresses that even during the Cold War Era – a period in history one could argue could typically be described in a narrow, military way – the exact 'meaning' of security changed over time. Moreover, Fierke describes a process of broadening and transformation of the concept of security (see also Buzan, Waever and De Wilde 1998; Nayak and Selbin 2010) and notes that security 'is essentially a contested concept'.

It is interesting to see whether technological developments, leading to the coming into existence of cyber space, indeed change the nature of war and consequently affect the nature of security. If so, this would pose a great challenge to the study of international relations in the 21st century. Until now no scholars of international relations have faced this challenge and satisfactorily investigated the above mentioned assessment. Potential effects of cyber are almost completely neglected.

This thesis takes on this challenge and tries to fill in this important gap in international relations literature. First it will theorize whether technological developments and threats from cyberspace indeed change the nature of war. After that it will focus on the effects of these developments on the closely connected concept of the nature of security. The research question of this thesis will be:

To what extent and in what way does the cyber revolution change the nature of war and security in the 21st century?

To answer this research question, the following sub-questions will help to structure the research process:

- How do current nature of war theories assess the influence of cyber on war and conflict?
- How do security studies assess the influence of cyber on the concept of security?
- What would be the effect of cyber war on the position and power of state and non state actors?
- What would be the effect of cyber war for critical infrastructure?

Finding an answer to the main research question has both scientific relevance and societal relevance.

1.4 Scientific Relevance

Its scientific relevance clearly lies within the current gap in the scientific literature that it tries to fill in. As one of the first attempts in the field, this thesis makes an effort to assess in what way the cyber revolution has changed the nature of war and security in the 21st century. In doing so, it will provide us with further understanding on the logic behind cyber conflict and cyber warfare. For example it will shed light on the empowerment of non state actors by cyber developments, the specific mechanisms that drive cyber attacks and the main targets it aims at. This will help indicate future challenges and thus help us evaluating the value and explanatory power of current international relations theories in the light of the cyber revolution. This thesis will bring up possible improvements for existing theories and will provide starting points in order to develop new ones. It is a step to prepare our discipline for the cyber era.

1.5 Societal Relevance

This mission to broaden our scientific knowledge directly leads to the societal relevance of this research project. It is likely that the ICT-revolution and the birth of cyberspace is still at its early stages. Our knowledge and technological innovation does not stand still, and grows every day. And

whether we like it or not, the impact of these innovations on our daily lives will most likely increase rapidly as well. Technology and innovation have the unique characteristics that it both makes our lives easier and more joyful, as well makes them potentially more insecure. Cyber war, cyber conflict, cyber theft and cyber criminality are as much part of the future as the unimaginably advanced tablets, computers and other devices we are all so happy with. In order to also stay safe in the future it is key to develop our knowledge in this domain of international relations so future policy makers know what to watch out for and how to cope with possible threats from cyberspace.

1.6 Thesis Outline

After this introductory chapter, this thesis will continue with the second chapter which is on the theoretical background of this research project. This theoretical part will sketch the development of war and conflict through the ages and will try to fit in the recent cyber revolution into this picture. It then tries to theorize on how the concept of the nature of war has or has not changed over time. After this the nature of war is linked up with the nature of security, and the specific connection is drawn with developments in cyberspace. The theoretical chapter will wrap up by bringing up two clear hypotheses that help us answer the research question. The third chapter will consist of a methodological chapter in which the modus operandi of this project is further explained. Here a comprehensive description of the research design of the thesis can be found as well as an operationalization of relevant concepts. Consequently the fourth and fifth chapter will entail the empirical case study of this project, leading towards the final conclusions and potential fields for further research as formulated in the concluding sixth chapter.

2. Theoretical Framework

2.1 Introduction

By nature, the study of International Relations (IR) from its very beginnings onwards has focused on the concept of war, the nature of war and the transformation of warfare through times. Where most scholars tend to agree with Carl von Clausewitz's rather basic notion that 'war is the continuation of *Politik* (translated as either politics or policy) by other means' (Von Clausewitz, 2004), disagreement prevails on almost all other subjects in the study of war. Debates on war and warfare have been around ever since people actually started writing down their accounts of the world around them. For example, ancient Greek historian and philosopher Thucydides (460-395 B.C.) probably is one the oldest and best known contributors to the theory of war. His *Melian Dialogue* on the Peloponnesian War between Sparta and Athens (431-404 B.C.) is generally perceived to be one of the founding pieces of International Relations theory (Alker, 1988).

The world has not stood still since the Peloponnesian War. Contrarily, the last two thousand years visions on war and all related concepts have changed dramatically. As a result, scholarly attention to this field never diminished, but increased instead. For example, the important fact that nowadays wars are generally conceived to be an interstate phenomenon is not something that has been around ever since the Peloponnesian War. In each period of time war can be recognized by its specific contextually and temporally bound characteristics; through time wars can generally be distinguished by their involved actors, goals, means of warfare and how they are financed (Kaldor, 2013, p7).

In the times of the ancient Greek empire no international 'system of states' was in place. The international system of states is a relatively young concept. It is only since this Peace of Westphalia (1648) and the related coming into existence of the *Westphalian System* that we can actually speak of the beginning of the international system of states. The most important consequence of the Westphalian System is the recognition of states authority and sovereignty and the state as the exclusive and legitimate bearer of the monopoly of violence and the use of force. This has major

consequences: from this moment on war has become an instrument of states to pursue their interests in inter-state conflict. Other main cornerstones of the Westphalian system are the principles of self-determination and state sovereignty, the principle of legal equality between states, and the principal of non-intervention. Since this peace agreement we can speak of a system of states, and subsequently we have been witnessing wars between states instead of wars between empires, duchies and so forth.

The year 1648 marks the birth of an era of inter-state war, guided by international laws and ethics of war that developed in the 17th and 18th century. Wars are a means of states to pursue their interests. The way we nowadays view war is a product of these evolutions of the modern state in Europe between the fifteenth and eighteenth century (Kaldor 2013, p.15).

The era of inter-state war and the development of the modern state has played an crucial role in the contributions and views of military theorist and German General Carl von Clausewitz (1780-1831), best known for his famous work *Vom Kriege* (On War). His seminal work on the nature of war is closely related to the concept of inter-state warfare. The most salient conclusion of *On War* is that the very nature of war (of war being interactive, violent and inherently politically driven) is unchangeable and 'tends towards extremes'. According to Clausewitz the only change that could occur over time is a change in the way wars are fought – so the mode of warfare. *On War* is best known for its dialectic analysis of war resulting in Clausewitz' two ideas of war.

On the one hand Clausewitz brings up the concept of 'Real War', or war as a strictly political instrument for states within the spheres created by the international system of states. In the situation of 'Real War' states are using their military power in order to pursue their own interest, but they are doing so within the 'rules of the game'. Moreover states in the case of 'Real War' are portraying prudence and are best to be qualified as rational actors in the international system pursuing limited goals (and thus are clearly not revisionist). Analyses in IR theory that are based upon this vision of Real War are numerous; the most important being the realist school of thought. The realist theory of the balance of power in international relations perfectly fits this world view as sketched.

However this is not the complete picture one can extract from On War, Clausewitz clearly juxtaposes this situation of 'Real War' with the extreme, ideal concept of 'Absolute War'[2]. 'Absolute

[2] Absolute War is not to be confused with Total War, since they are two different concepts. This will be dwelled

War' completely opposes the foundations of 'Real War'. In this situation the 'rules of the game' that clearly guided the situation of 'Real War' are completely put aside. Limited wars evolve into total wars, and limited aims grow into revisionist ones. The situation of 'Absolute War' does not grow out of nothing, instead Clausewitz developed a theory in which he lays down his views on how 'Absolute War' can be the logical end state of 'three reciprocal actions', that together are able of creating a negative spiral toward 'Absolute War'. This chapter will investigate this process more in depth, but for now it is important to underline that Clausewitz does not think it is likely that Real Wars will evolve into Absolute Wars in reality. While it is theoretically possible they will evolve into Absolute Wars, they almost never do[3]. This is a result of the fact that wars are almost never fought in their purest form, because they are subject to all kinds of hindrances which he calls 'friction'.

As described earlier, Clausewitz – among others – is a staunch believer of the unchangeable nature of war. According to proponents of this view, only the way wars are fought changes and not its very nature. Discussions on the nature of war can have profound implications for IR theory. Authors like Kaldor (2013) air their views on the radical changes in the nature of war, and – importantly - also stress that these changes of the nature of war challenge our current concept security and of related IR theories. If, for example, the nature of war changes in a way so that states no longer are the primary actors, then is there still value in realism? Many scholars have contributed to similar studies on the transformation of war, or as it is more commonly called the 'Revolution in Military Affairs' (RMA). This thesis's main interest lies within the effect of the revolution in information technologies (IT) and the connected 'new' domain of cyberspace as part of this Revolution in Military Affairs. It focuses primarily on the possible effects of these cyber developments on the changing nature of war and ultimately on its consequences for security in IR theory. The state centric visions of Clausewitz are used as a starting point; his claims on the unchanging nature of war are further investigated. Special attention will be put on the mechanisms that theoretically force Real Wars into becoming Absolute Wars. This is important because this thesis is interested in the possible reinforcing effects of the RMA (and more specifically cyber!) on the

upon later in this thesis

[3] Clausewitz himself does not mention a single example of an Absolute War in his book. Following his theory we could say that until now there has never been an Absolute War in Clausewitz's terms.

negative spiral toward Absolute War and radical change in the nature of war. If indeed this is the case, this chapter will subsequently challenge the value of realism in this 'new era' of cyberspace, given the fact that basic presumption of realism (for example state centrism) might no longer hold in the future. This chapter will then wrap up with shedding light on the effects of this on the concept of security and how this concept is also subject to change in this new era. It all tries to answer one question: do cyber developments change the nature of war and security and do we need a new theory in IR to cope with this?

2.2 The Nature of War is unchangeable: Clausewitz

In 1832 the seminal work *Vom Kriege* (On War) of German general and military theorist Carl von Clausewitz was posthumously published. In this notable monograph, which unfortunately remained unfinished, he points out that war is essentially 'a social activity' (1976). War involves mass mobilization and organization of people – predominantly men, not women – with the sole goal of inflicting (physical) damage to an adversary. 'War is the continuation of *Politik* (translated as either politics or policy) by other means'[4], and this inner nature according to Clausewitz is unchangeable. Only its character – the method of warfare and the way war manifests itself – can be subject to change. The very core of the nature of war is interactive, violent and inherently politically (read state) driven. The nature of war itself captures its unchanging essence, nature of war doctrine explains exactly those things that differentiate the concept of war from concepts in which war is absent. Gray (2010, p.6) agrees with this notion and states that 'many people confuse the nature of war with its character. The former is universal and eternal and does not alter, whereas the latter always is in flux.

As often noticed the concept of war as introduced by Clausewitz is closely related to the evolution of the modern state in Europe between the fifteenth and eighteenth century (*ibid.* p.15). This evolution of the modern state went through several different stages in time. Each of these stages had their own, different mode of warfare, strategy, techniques and means of warfare. Since the contributions and thoughts of Clausewitz are so closely bound with the historical development of the

[4] Some authors such as Holmes (2014) point at the misinterpretation of this famous sentence of Clausewitz. According to Holmes Clausewitz statement – if properly translated – would be 'War is the continuation of Politik *with* other means'.

modern state, Clausewitz almost solely speaks about wars between states (in order to serve a specific state interest) and not about war within states or wars concerning non-state actors.

An important effect of the creation of the modern state was the establishment of standing armies under the control of a state's authority, and subsequently also the moral and legal separation between combatants and non-combatants (see for example Walzer 2006). This state control on the instrument of violence marked the finalization of the process of the state's monopolization of legitimate violence. As a result states interest and the use of violence (read war) became strongly connected. War from this moment on could be seen as a legitimate tool in a state's toolbox in order to pursue its vital interests, or as Clausewitz would state it: this legitimate monopoly of violence gives states the possibility to 'continue its politics by other means' (Kaldor, 2013). The goal of war - importantly in this case referring to his concept of Real War - could be described as tool to pursue the rational interests as formulated by states. When Clausewitz speaks of 'the Political' he clearly is referring to the state as main actor, as present after the Peace of Westphalia in 1648 (*ibid.*).

2.2.1 Clausewitz's Trinitarian Model and 'Absolute War'

Clausewitz considers war to be a pure social activity, that links different emotions (such as reason, passion etc.) to the three different levels of the modern state: the population, the army and the government. This three layered approach is often referred to as the 'Trinitarian model'.

Clausewitz's Trinitarian model of war is of major importance, because it enables us to understand one of his most commonly referred to (and also commonly misunderstood) concepts, the concept of 'Absolute War'. According to Kaldor (2013, p.23) the concept of 'Absolute War' is best interpreted as a Hegelian abstract or an ideal concept, or as some say a Platonic Ideal, a 'pure theoretical abstact.'. Clausewitz himself calls it a 'logical fantasy'.

A state of 'Absolute War' or the revisionist aim of totally disarming and destroying an adversary ('rules of the game' have disappeared) can be the logical consequence or end state of the inner logic of the three different tendencies in war – the tendencies that together constitute the Trinitarian model. These three tendencies can be witnessed empirically and Clausewitz calls them the 'three reciprocal actions'. These three reciprocal actions together can – in the 'ideal situation'-

eventually create a downward spiral toward ‘Absolute War’.

First, at the political or rational level one can see that a state almost always meets resistance in achieving its objectives. Therefore, in order to be able to successfully achieve what a state wants to achieve, a state always has to press harder and use more force.

Second, at the military level the main aim should always be to completely disarm the opponent to be sure that they will not have a chance of a launching a potential counter-attack.

Third popular feelings and sentiments in society or of major importance, since war creates emotions that might end up to be uncontrollable.

As a result of the reinforcing effect of these three reciprocal actions, the ‘rules of the game’ have vanished, and a situation of Absolute War arises. It is important to once again mention that for Clausewitz Trinitarian model to work out, one has to first and foremost accepts the primacy of the concept of the state. This is because the concept of the state is the start point of his reasoning. Without the presence of a state, the underlying foundation of his reasoning disappears. This is interesting to keep in mind when studying the effects of cyber. As we will see later on in this chapter, it is sometimes argued cyber developments seriously challenge the primacy of the state.

As described, the concept of Absolute War is oftentimes misunderstood by a majority of scholars referring to his works. Although Clausewitz states that wars ‘tend to end up in extremes’, the end situation of Absolute War is in reality not likely to occur (and in fact until today has never occurred). Clausewitz himself indicates two main reasons why war almost never ends up in the extreme situation of Absolute War. His first argument for this thesis is that situations might arise in which political objectives of a state are limited and not revisionist at all, or in which popular backing of a state’s action is lacking. His second main argument is that war as a concept is never experienced in its purest form. In real, war is always confronted with ‘friction’. Basically this friction can be everything that makes war in practice different to war ‘on paper’. One could think of weather conditions, disobedience, rebellion, poor logistics etc. It is exactly because of this friction that Clausewitz introduces the concept of ‘Real War’. He introduces this concept which he calls ‘friction’ to ‘describe the effect of reality on ideas and intentions in war’. Real War is the logical result of the tension between the inner tendencies of war that lead to ‘Absolute War’ and the political and practical

constraints that withhold wars to grow into the idealistic form of 'Absolute Wars'.

Here it is however important to stress that Clausewitz (1984) himself describes the possibility that Real Wars actually do evolve into Absolute Wars – so that the three reciprocal actions in fact do work. According to him state policy determines the main lines along which wars move, so if political tensions carry very powerful character, and if ample military means are available it is very well possible that rational political means may disappear and be replaced by revisionist ones.

Now that we have taken account of the inner logic of Clausewitz's Trinitarian model and the surrounding political and practical constraints, an important question arises. Clausewitz's approach is heavily (if not completely) based upon a purely state-centric vision. It is solely because of this state centric character of the international system that his Trinitarian model works the way Clausewitz introduces it. And this is vital: what would be the effects of this in the case of a weakening or maybe even complete breakdown of this state centric paradigm[5]? It would be interesting to see whether in a situation of the breakdown of the state and thus the likely absence of the Trinitarian model, there would still be a possibility of a negative spiral leading to Absolute Wars. Also the question arises if the concept of friction would still apply. In short: Do states and non state actors behave alike?

2.2.2 Clausewitz's Trinitarian Model Challenged?

This analysis on the concept of war and the inner tendencies of war that do or do not lead to 'Absolute War', touches upon a core part of the question this thesis tries to answer. As the analysis shows, Clausewitz focuses on a strictly state centric view of international relations. In this very focused view Clausewitz developed his theory and its predictions. It is interesting to try and assess whether these views do actually still apply – or in other words: is the nature of war really unchangeable (and thus is Clausewitz still useful in today's world?).

Watts (2004, p.1) also recognizes this potential challenge and puts it as follows: 'There has been growing discussion on the possibility that technological advances in the means of combat will produce fundamental changes in how future wars will be fought'. Given the fact that Clausewitz'

[5] Keegan (1993) interestingly notes that 'Clausewitz assumed the existence of states, yet war antedates the state, diplomacy and strategy by many millennia'.

theory of Absolute War is based upon his strictly static Trinitarian model of war, it would be interesting to see what would happen if the IT-revolution and the birth of cyberspace indeed radically change the static character of the international system, for example by a breakdown of the concept of states as Clausewitz describes them. Would it then still be possible that the spiral towards absolute warfare is slowed down or even reversed by 'friction' experienced by one of the three parts of the trinity? Would this create a situation in which the theoretical ideal concept of Absolute War becomes a real possibility? Partly answering this question, Kaldor (2012, p.27) states that new developments such as nuclear weapons (and although she doesn't name them explicitly herself, potentially also developments from cyberspace) in theory 'could wreak total destruction without friction'. And this is of major importance when one considers the fundament of Clausewitz's theory on why the nature of wars 'never change'. If we have a closer look at the roots of this view on the unchanging nature of war, we can come to an important assessment. The sole reason why - according to Clausewitz – only the way of warfare and not the nature of war can changes, is because the foundation of his inner logic behind his theory of war never changes. It is deeply rooted in his conception of war as 'continuation of *policy* by other means' by a specific *state*. Because in his view states are and will always be the major continual shapers of the international arena, the nature of war that automatically follows through the Trinitarian model will always be the same. War is an unchangeable concept. Obviously, Clausewitz did not get beyond the important limits of this purely state-centric assessment of the world he was living in. This can have profound implications, for if the very foundations of his theory have changed, what are the effects of this on the nature of war? Imagine that Absolute War in fact would occur (for example as a result of developments in cyberspace) and the rules of the game would indeed have disappeared - can we then still speak of an unchanged nature, or has this very nature changed as well?

2.3 The Nature of War is changeable: the Revolution in Military Affairs

Not everyone agrees with Clausewitz's notions of the unchangeable nature of war. One of the staunchest critics of this Clausewitzian notion is Mary Kaldor (2013). In her book *Old and New Wars* she strongly argues against the unchangeable nature of war. Kaldor (*ibid.* p.15) argues that war is 'strongly contextually bound' phenomenon. She gives an overview of how wars evolved on the European continent: it all started with the limited wars of the seventeenth and eighteenth centuries, followed up by the revolutionary wars of the nineteenth centuries that created the foundations of the total wars of the twentieth century ending in the Cold War. During these different periods in time – according to Kaldor – the wars in themselves were different. The goals, their organizations, their logics and most fundamentally their nature was different. All these different wars really only had one thing in common, they are 'a construction of centralized, 'rationalized', hierarchically ordered, territorialized modern state'. According to Kaldor, these are 'Old Wars' (as opposed to 'New Wars').

Mary Kaldor touches upon a really interesting point when she stresses the contextually bound character of wars, and especially the fixation of the relationships between war and the modern state. As we can clearly see Clausewitz does not seem to include phenomena of non-state warfare in his work *On War*. It could very well be the case that Clausewitz did not even think about other actors than states to be involved in war. He was living in the heydays of great, total wars [6] on the European continent where state power seemed to be the only thing that counted – take for example the Napoleonic Wars. There was no real need to consider non state actors to be of importance in a theory on the nature of war. But didn't that change since Clausewitz's times? According to Kaldor it did, and she names her concept 'identity politics' and the related breakdown of central government to be a decisive difference between 'Old Wars' and 'New Wars.

Kaldor's contributions can be put into a broader debate, namely the debate on the Revolution in Military Affairs (RMA) as mentioned already in the introduction of this chapter. This thesis will now proceed with analyzing the RMA. It will focus not on Kaldor's insights on identity politics, but

[6] Although these Total Wars of the 20th century did not equal the ideal concept of Absolute Wars, they nevertheless came as close as be conceived (Kaldor 2013, p.27) In reality, Total Wars are just one step before Absolute War

instead primarily concentrate on the IT-revolution and the related field of cyberspace. The goal of this analysis is to investigate whether the IT-revolution and cyberspace affect the changing nature of war, and in what way. Ultimately the goal of this is to put Clausewitzian state centric accounts and the rationale of Real and Absolute War to the test.

2.3.1 The Revolution in Military Affairs and the IT-revolution and Cyberspace

Whether as Clausewitz stated war is an unchangeable concept, or as – among others - Kaldor stresses that the nature of war indeed is (and always has been) subject to change at this moment is not of major importance. Similarly, the Revolution in Military Affairs (RMA) may or may not have changed - in Clausewitz's terms - the characteristics and not the nature of war. This is a rather empirical and not so much theoretical question. Therefore it will be assessed later on in this thesis.

For now this paragraph will concentrate on the arguments of proponents of the view that military affairs indeed have changed and are still subject to change as a result of technological developments. The possible effects of changes in (the nature of) war can have important implications for how we conceive war, and for the connected IR theories and the crucial concept of state's security. Many scholars have contributed to studies on the transformation of war, or as it is more commonly called the 'Revolution in Military Affairs'.

The Revolution in Military Affairs (RMA) is a theory about the future of warfare, nowadays often connected to the revolution in information technology (IT). Many authors refer to this RMA in order to discuss possible transformations in the nature of war. Although scholars have identified different areas of focus when it comes to RMA, the victory of the United States army in the 1991 Gulf War against Iraq can be seen as a good example of the value of increased information technology as described in RMA. This war clearly demonstrates how American superior technology greatly reduced the relative power of the Iraqi army by improving technology and effectiveness of weapon systems. It highlights the evolution of weapons technology, military doctrine and organization. For example the recent developments of unmanned aerial vehicles (UAVs), drones, satellites, robotics and biotechnology are clear signs of the RMA.

Some authors such as O'Hanlon (2002) and Kagan (2003) disagree with the notion that due to

IT-revolution we are also witnessing a revolution in military affairs. According to them, most of the techniques we are linking to the RMA and are nowadays using in fact already were initially developed before the IT-revolution and the existence of internet. This does not mean these and other alike minded scholars necessarily do not believe in the possibility of a revolution in military affairs to take place. For example Rogers (1995) makes a distinction in the Revolution in Military Affairs (RMA) and what he says historians call a military revolution. Military revolutions throughout history are known for their nature of having intense consequences even outside the realm of the military. According to Rogers RMAs are precursors of military revolutions, and in order for RMAs to become military revolutions they need to change not only the military realm, but instead all of society and the balance between defense and offense (*ibid.*). Whether or not the IT-revolution in warfare fulfills this specific definition of an RMA at this point will not further be dwelled upon. Instead this thesis will assume the IT-revolution has profound consequences, and is therefore nevertheless valuable to be studied more in depth.

The effects of the revolution in information technology can have major impact on the nature of war. As an effect of the this RMA and IT-revolution, war can change significantly, not only empowering new techniques and strategies, but more importantly also new actors participating in wars. Information technologies seem to be increasingly shaping possibilities for non state actors[7] to become a player in the international arena, contributing to what some call the 'breakdown of the state' and the coming into existence of 'super individuals'. This potentially poses tremendous challenges for states and their security, and is disturbing our most common and basic views on what war is, how it is fought and by whom it is fought. Also it causes major problems for war conventions and the law of war. As an example, with the uprising of non state actors becomes increasingly difficult to distinguish between combatants and non combatants (Walzer, 2006). Kaldor (2013, p.3) even states that 'the advent of information technology is as significant as was the advent of the tank and the airplane, or even as significant as the shift from horse power to mechanical power', and she further adds that this will have profound implications for the future of war(fare).

[7] Examples of non-state actors are for instance transnational terror groups such as Al-Qaeda or transnational organized crime groups.

Challenging the state-centric Trinitarian theory of war as proposed by Clausewitz, Martin van Creveld (2009) in his book *The Transformation of War* brings up his own non-Trinitarian theory of war. Van Creveld does so, because he strongly believes that conflicts nowadays cannot be properly studied using Clausewitz's framework. It is too narrow and state-focused and therefore is unable to deal with the study of conflicts involving one or more non-state actors.

Van Creveld's non-Trinitarian model exists of five indicated 'issues of war'. These five issues together form a typology of modern war and according to Van Creveld provide the tools in order to be able to explain modern conflict:

1. *By whom war is fought* – whether by states or non-state actors;
2. *What is war all about* – the relationships between the actors, and between them and the non-combatants;
3. *How war is fought* – issues of strategy and tactics;
4. *What war is fought for* – whether to enhance national power, or as an end to itself;
5. *Why war is fought* – the motivations of the individual soldier.

As one can see this non-Trinitarian notion of war radically changes the concept as introduced by Clausewitz. Van Creveld developed this typology because of the vast increase in low-intensity conflicts (LICs) since 1945, in which powerful states often end up losing. He furthermore argues that we are witnessing 'a decline of the nation-state', commonly described to be his 'dying state' thesis (Van Creveld, 2004).

It is now interesting to investigate what the influence of the IT-revolution and cyberspace is on this potential 'breakdown of the nation-state'. And more importantly and strongly connected to this potential impact of cyberspace, is its potential effect on the nature of war or in other words: does Absolute War as formulated by Clausewitz become more likely?

Threats originating in cyberspace are not to be overestimated in any sense. As referred to in the introductory chapter of this thesis, influential people such as the US Director National Intelligence have named cyber threats to be topping the lists of most important threats to US and international security. According to him 'more and more state and non state actors gain cyber expertise, and its

importance and reach as a global threat cannot be overstated' (Global Threat Assessment, 2013, p.2). Bendrath (2001) points to a study by the US National Security Council stating that 'Tomorrow's terrorists are able to do more with a keyboard than with a bomb', and Eriksson and Giacomello (2006, p.226) add on this by quoting Former US Homeland Security Director Tom Ridge: 'Terrorists can sit at one computer connected to one network and can create world havoc – [they] don't necessarily need bombs or explosives to cripple a sector of the economy, or shut down a power grid' (Green, 2002). The most extreme examples have also already been provided, some people even warn for a 'Cyber Pearl Harbor' or 'Digital 9/11'.

Eriksson and Giacomello (2006, p. 225) are convinced that the very conception of this new cyber threats are a direct result of the fear of increased vulnerability and loose of control which is the result of the transition from the industrial to the information society.

There are a lot of scholars who stress the transnational, network-based nature of cyber warfare and cyber threats (Eriksson and Giacomello, 2006; Keohane and Nye, 1998; Lin 2010). The players within cyberspace are different to the ones operating outside of it. Adversaries are usually loosely organized in networks that consist of relatively independent parts that can be individuals, organizations, groups and also states. These loosely knit networks are usually formed for a by a certain situation, and are afterwards quickly dissolved – sometimes even before a potential attack has been indicated and attributed (Eriksson and Giacomello 2006, p.227). This network oriented basis of threats in cyberspace highly increase the likelihood of asymmetric warfare. Cyber threats usually involve a broad range of adversaries and targets, both state and non state (Campen et al. 1996). In order to sum up the unique characteristics originating in cyberspace, Choucri (2012, p12) developed a typology of the characteristics of cyberspace:

- *Temporality* – replaces conventional temporality with near instantaneity
- *Physicality* – transcends constraints of geography and physical location
- *Permeation* – penetrates boundaries and jurisdictions
- *Fluidity* – manifests sustained shifts and reconfigurations
- *Participation* – reduces barriers to activism and political expression

- *Attribution* – obscures identities of actors and links to actions
- *Accountability* – bypasses mechanisms of responsibility

As one of the most important results of this unique features that characterize cyberspace, boundaries between international and domestic, private and public, states and non-states and private and public are heavily impacted (the physicality and permeation). The sovereignty of states is seriously challenged (Van Creveld 2007, Eriksson and Giacomello 2006,). However, according to some authors like Eriksson and Giacomello this primarily entails internal sovereignty (effective and legitimate control of national territory and its inhabitants) and not so much external sovereignty (formal recognition of independence in the international system of states).

As we can see several scholars in IR make the case that the RMA and specifically the IT-revolution and the rise of cyberspace, seriously challenge the primacy of states and the static system that goes back all the way to Peace of Westphalia in 1648. Whereas during the last centuries states without doubt were the main actors of interest in international relations, due to recent developments power relations are changing. This does not mean that states no longer count in IR, it simply suggests that states are not the only relevant actors anymore. Due to the IT revolution a new domain of cyber found its existence. As an important effect of this cyber domain the traditional unbridgeable gap between the power levels of the state and all other potential actors in IR is being bridged, at least for an important part. One can easily understand that in the past era of total wars it was literally impossible for non state or transnational actors to acquire the same levels of military and economic power as states were capable of. In the past, it was just impossible for non state actors to establish armies or develop and finance expensive and demanding military technologies. This is something that has changed ever since, and although heavy debate still exists on the exact implications of this, most scholars tend to agree on this. The only thing they disagree on are the effects and the magnitude of these developments.

This image brings us to a very interesting point. Imagine a situation in which indeed as a result of the IT-revolution and cyberspace these differences between state and non state actors diminish. What consequences would this have on the nature of war; would Clausewitz notions on the

unchangeable nature of war still hold? This is an important question to be taken into account, given the fact that – as mentioned earlier – influential IR theories are based on the core assumptions of Clausewitz' static analysis on wars, and the rationale behind 'Real Wars' evolving into 'Absolute Wars'.

2.3.2 Hypothesis One: The Actor-hypothesis

Unfortunately, it is impossible to directly test this overarching expectation that Absolute Wars are more likely to occur as an effect of cyber capabilities, The reason why is simple: Absolute War has never occurred in real. What we can do instead, is deriving hypotheses that can shed light on important components of this overarching assessment.

The above provided analysis on the possible changing effect of cyber on the nature of war leads us to the first hypothesis that can be tested in this thesis. As described by Van Creveld (2004) and Choucri (2012), possibly the most expected change due to cyber is that the traditional leading role of state actors in international relations is seriously challenged. It is assumed that cyber capabilities empower non state and hybrid actors at the cost of the relative position of state actors. If this is true, we would expect that the differences in cyber capabilities between state and non state actors are smaller than the differences in conventional military capabilities. Therefore hypothesis one is as follows:

H1: When it comes to the cyber war, the differences in cyber capabilities between state and non state actors are smaller than the differences in conventional military capabilities

2.4 Challenging the implications of Clausewitzian theory: a case against Realism[8]

Realism is one of those theories in IR that have been of major importance the last decades and are greatly based upon Clausewitzian accounts of the nature of war. Realist thought is mainly developed by the influential works of scholars such as Morgenthau, Waltz and Mearsheimer and perceive rational

[8] It is specifically chosen to introduce a case against realism and – although they have many important similarities – not against liberalism. This is done because in general liberalism tends to 'emphasize the positive outcomes of interdependence and interconnectedness, rather than the increasing vulnerability and insecurity that might ensue' (Eriksson and Giacomello, 2006)

states to be the only dominant and relevant actors in IR. Given the fact that the aforementioned analysis possibly seriously challenges this hard core of Clausewitzian and Realist thought, do these insights still have value in the era of cyberspace?

In international relations theory the theoretical views of realism stand out as one of the most influential schools of thought in recent history. This school of international relations theory emerged as a direct effect of the inter-state war years the 20th century. The tradition of realism is centered around four important, basic assumptions:

1) The international system is anarchic;

   Realists believe that the international system is anarchic. This means that there is no centrally organized actor above states that is capable of regulating interactions among states. As a direct effect states are responsible for their own interactions (and effects of them), since no higher controlling entity exists or can exist. The international system is a self-help system.

2) States are the most important actors;

   Relists believe that the international system is an international system consisting of states as the main actors[9]. This means that whereas they accept that in the international relations arena other non-state actors can and in fact do exist, they are never in the position of harming the central position of states. Only states have the organizational capacity to remain strong enough to survive.

3) All states in the system are unitary and rational actors;

   Realists believe that all states in the international system or behaving insofar they can pursue their particular self-interest. They are unitary in the way that they speak and act with one voice. Therefore it is important for states to attain as many resources (and thus power) as possible. Increasing relative gains (vis-à-vis other states) is what matters.

[9] Realism is primarily focusing on the role of 'big states' in the international system, and seems to be less interested in 'small states'. This is interesting also for this thesis, since it is very well possible that cyberspace influences them differently as well.

4) The primary concern of all states is survival in the system.

   Realists believe that the most important objective of each state is the question of how to survive in the international system. In order to do so states build up military organizations to be able to survive, which inherently creates a situation in which states become entrapped in a security dilemma[10]. Power measured in terms of military capabilities and the associated striving for security is therefore the main driving force in international politics.

One of the most important concepts of realism (that directly results from the four aforementioned assumptions) is the international distribution of power, or as realists call it the polarity of the international system. They generally distinguish between situations of unipolarity (one hegemon), bipolarity (two powers or power blocks) and multi-polarity (three or more powers or power blocks).

In line with the concept of the distribution of power in the international system, realists bring up the intensively studied theory of the balance of power. The idea behind the balance of power is that the national security of an individual state is increased when power and military capabilities in the system are distributed in a way so that no one single state on its own is powerful enough to dominate all others. If a situation occurs in which one state in fact does gain an unacceptable relative increase in power vis-à-vis other states, the theory predicts that states would start to balance against the state that increases its power. Among different factions within realism there is a big debate on how the polarity of a system influences the different tactics states use to restore the balance of power.

As one can see realism's core is pretty much all about one thing: states. This sharply contrasts with the analysis in the past paragraphs in which this thesis showed the debates around the 'breakdown of the state' views. Eriksson and Giacomello (2006, p.229) try and investigate how proponents of realism would handle the challenges that states are confronted with as a result of cyberspace. According to them, realists might voice that in principle they do not see any point in revising their theories to understand these developments. Even in the digital age states are still be considered as the

[10] The 'security dilemma' refers to a situation in which actions by a single state that are intended to increase its security (such as alliance or more advanced weaponry) can lead to other states responding similarly. This can create increased tensions in the international state system even though no one really desires this (Jervis, 1978).

main and most important actors in the international system. Also with the developments of the IT-revolution and cyberspace, non-state actors will not be capable of really challenging state's authority. They would frame these developments exactly the way they did with developments in the past, such as globalization, complex interdependence and trans-nationalization. According to most realists, these developments need to be seen strictly as epiphenomenal, maybe affecting the policies and internal structures of states, but definitely not undermining the core feature of the international system – anarchy. Therefore, states are and remain the main and most important actors in international relations, and also in the new cyber era, no non state actors (like super individuals or transnational terrorist groups) are capable of seriously threatening the security of the state. Therefore, realists clearly support a narrow, strictly military definition of security, herewith denying that non-state actors are able to really attain any serious degree of military power.

But is this really the case? Especially when we recall and keep in mind the statements of several high ranked US officials on the future possibilities of a 'cyber 9/11' or an 'electronic Pearl Harbor', we should critically reflect on the aforementioned realist analysis and subsequent notion of security. The fact that until this moment no cyber attacks with such agonizing effects have taken place, doesn't provide any guarantees. The Revolution in Military Affairs goes on, arguably only amplifying and not limiting the possibilities and consequences of cyber in the future. A further analysis on the possible consequences of the empowerment of non state actors on the nature of security is needed.

2.5 The IT-Revolution, Cyberspace and the Nature of Security

Within the study of international relations there is no universal definition of the concept of security. Although the exact meaning of 'security' is contested (Fierke, 2007), there is consensus that studying and discussing the concept is of major importance. Security is a multidimensional concept that has widely been used to justify radical state's policies like 'suspending civil liberties, making war, and massively reallocating resources' (Baldwin, 1997).

Within this IR-subfield of security studies, we can witness a strong division between the traditionalists and the 'wideners'. These opposing sides differ strongly on their conceptualization and the meaning of security. In the introductory chapter of this thesis we already shortly touched upon this

debate in security studies. On the one hand we find traditionalists that strictly adhere to a traditional, rather narrowly formulated meaning of security. They see security in a solely military way, focusing on the study of military threats and vulnerabilities of predominantly states and their core interests.

On the other hand, the 'wideners' disagree with this inclination on the narrow, military character of security and tend to 'widen' the meaning of security, so that the study of security doesn't necessarily only include the military notion of 'threats' but also fields like environmental, health and food security. Also they pay specific attention to the subjective character of 'threats'[11], stressing that instead of being objective threats are socially constructed. These views have become known as part of the school of critical security studies (CSS).

2.5.1 Traditional Security

The traditional security paradigm is rooted in a realist construct of security, in which security is exclusively considered to be a static concept – or as this is more commonly called in the field of security studies: the state is the referent object of security (Walt, 1991). As is the case with realist theory, the traditionalists views on security were most prevalent during the decades of the Cold War. During the Cold War as a result of a conflict between two major power blocks – the United States and the Soviet Union – states relied for their security on what realists call 'the balance of power'. Due to the balance in military capabilities between the two super powers, no one of them was powerful enough to destroy the other. This situation of relative stability created security for both power blocks' core interests. According to Owen (2004) 'traditional security relied on the anarchic balance of power, a result of the military build-up between the United States and the Soviet Union, and on the absolute sovereignty of the nation-state'. States are conceived to be striving for absolute power, and security provides them protection against invasion and harm done to their core interests.

On the side of the proponents of the conventional and rather limited military conception of the security, we can find for example Lipmann (1944) describing security to be 'the capability of a country to protect its core values, both in terms that a state need not sacrifice core values in avoiding war and can maintain them by winning war. Others like Wolfers (1962) and Ullman (1983) expand on

[11] Not only wideners stress the subjectivity of threats, some traditionalists (for example Jervis) do this

this by introducing the crucial components of 'absence of threats' and 'decrease' in the vulnerability of a state's core interests. Stephen Walt (in Fierke 2007, p.13) summarizes these points and defined security studies as 'the study of threat, use and control of military force'. According to these scholars protecting security means a need to strongly focus on protecting the core interests of a state against potential threats.

2.5.2 Critical Security Studies

When the tensions of the Cold War decreased – most importantly with the fall of the Berlin Wall and the subsequent collision of the Soviet Union – the concept of security evolved. With the experiences of the Cold War fresh in mind, it became clear that the results of major power conflict maybe not so much affected the security of nation-states, but greatly harmed the security of individuals (Baylis, 1997). Baylis (*ibid.*) for example points toward the increase in inter-state conflict (i.e. civil wars) and the related 'threats to security' such as human rights abuses, diseases, hunger and poverty. As a result the realist, state-centric security paradigm has been challenged by scholars who want to 'widen' the narrow, military focused notion of security. Their efforts were mostly stimulated by critical interpretations of the territorially-bounded sovereign states and their related claims that state sovereignty equals security. Nowadays, they are known as part of the 'critical security studies (CSS)' approach (see Booth, 1991). The qualification of being 'critical' refers not to 'negativism' or 'being critical; but rather is an ethos that involves questioning knowledge and views that are taken for granted (*ibid*).

On the side of the supporters of the 'widened' vision on security, we for example can find Buzan (2000) with his views that 'the study of international security is more than a study of threats' , therewith introducing an approach that not only looks at the 'objective' character of exclusive military threats, but instead focuses on the how threats are in fact constructed and transcend the narrow military domain. The meaning of security is an outcome of a specific political and historical environment. Also Fierke (2007, p.4-5) is an important supporter of this 'widened' view on security. According to here the traditionalists definition of security is inherently politically and contextually bound, and even during the heydays of the Cold War the 'exact meaning' of security changed.

Critical security studies' aim is to enhance security (in the 'wide' sense) through emancipation. Booth (1991, p.319) states that 'emancipation theoretically is security'. He explains this by describing a situation in which wars and threats of war are constraining people to be free in carrying out their lives as they would want to. Security should be primarily involved with freeing people from physical and human constraints. Where military power might remove the physical constraints, emancipations removes the human ones. Therefore for example poverty, absent education and bad healthcare are as much part of security as military threats are. Given the *physicality* of cyberspace – meaning that it transcends constraints of geography and physical location – what would be the effect of cyberspace on the nature of security?

2.5.3 Bridging the Debate on Security: the domain of Cyber

It is often thought that the one's specific conception of security is tightly bound with whether one has state-centric vision on international relations or tends to criticize this realist paradigm. Also, it is often argued that scholars with a state centric inclination are more prone towards the narrow, military definition and that scholars with a less state centric vision tend towards a widened view on security.

Some authors in the field stress that while at first glance traditionalists and 'wideners' seem to be focusing on totally different conceptions of security, this need not necessarily be the case. Because it could very well be that in reality they are just emphasizing different aspects of the same shared concept. Further study on this is needed.

Baldwin (1997) is one of the authors who tries to disentangle these supposedly different 'sides of the debate', by trying to identify common conceptual distinctions that underlie the various – allegedly opposing - different conceptions of security. Stepping aside the specific details of his thoroughgoing analysis, his main conclusion is that security is 'not so much a contested concept', but moreover a 'confused or inadequately explicated concept' (*idem,* p.12). Increased attention should be given to more thoroughly explicate the concept of security when used in a particular scholarly debate - and if this is properly done – according to Baldwin one will see that the 'two sides that seem to oppose each other' in fact tend to come really close to each other.

For the purpose of this thesis it is at this moment not needed to go further into this specific

debate on the different underlying conceptual distinctions or similarities that Baldwin is introducing. Instead, this thesis will follow the main conclusion and advice of Baldwin (1997) and rather try to thoroughly explicate the concept of security as it is possibly affected by developments of the IT-revolution and cyberspace. In doing so, it is tried to transcend the simple black- and-white image of security and to come up with a explication of how security should be understood in the cyber domain. It tries to answer this vital question for this thesis, and comes up with a new, encompassing conception of security that incorporates the challenges that originate in cyberspace.

This is crucial. A new, encompassing explication of the concept of security is highly needed when one aims to study the effects of the IT-revolution and cyberspace security. The need for this new explication is rooted in the inherent character of cyberspace as mentioned before: cyber challenges the way the world of today is organized and literally connects worlds that until recently had no physical nor a digital connection. And interestingly in doing so, it seems to not only 'connects worlds' but also connects the two allegedly opposing – being the traditionalists and the wideners - conceptions of security when it comes to the cyber domain. When studying the cyber domain neither one of these two schools of thought is going to help you on its own.

As described before the developments in the cyber domain have far-reaching effects. Probably the most radical effect is that the primacy of the concept of the nation-state in the international arena has been seriously challenged as a result of the empowerment of non state actors. Whereas in the past states were undoubtedly the only relevant, powerful actors in international relations, cyber has minimized the gap between state and non-state actors.

Cyberspace is unique in the sense that it provides possibilities to physically attack using only digital means. As an effect of the IT-revolution almost everything in modern society uses technologies that are connected into broader networks. Cyber has the capabilities to penetrate into these systems and – if wished – can do harm. At first glance one might think of cyber attacks as mere attack on digital infrastructure (for example bringing down computer systems). It however is also possible to go one step further: invading in a system and consequently manipulate it so it works the way you want it to work.

As an effect, strictly 'military' speaking, cyber can be used just as any other conventional

weapon we know. By digitally entering hostile weapon systems and manipulating for example the guidance of a rocket launching infrastructure can turn threats, and possibly even backfire toward the eventual adversary. As an important example of the military use of cyber the case of the '*Stuxnet'*-virus is often described. In this case the United States and Israel allegedly penetrated into Iranian nuclear facilities and digitally brought it down. This 'conventional' use of cyber as a military weapon is however only part of the story. It maybe could be argued that if this would have been the one and only utility of cyber, the need for a new encompassing definition of cyber security would not be needed and instead the 'traditionalists views' would suffice. This is not the case.

Cyber has an important other side. Instead of using cyber purely for conventional warfare, cyber has far-reaching possibilities to be used in another way as well. Recently this focus on the possibilities of cyber to affect 'critical infrastructure' has gotten increased scholarly attention (see for example Cordesman 2002, Rajkumar 2010). The main point that is made in these debates is that using cyber it becomes substantially easier to attack critical infrastructure. Critical infrastructure is a term that is nowadays often used to describe assets of governments that are essential for the proper functioning of a society and economy. For example one could think of energy networks, telecommunication, water supply, agriculture, financial systems and so forth[12]. Because all these different parts of the critical infrastructure rely on highly advanced techniques, cyber has made them increasingly vulnerable. It is not difficult to understand that if a hostile state or individual is capable to for example bring down the financial system for a couple of days, the consequences would be unimaginable.

Maybe at first sight one would say that 'critical infrastructure' is equally vulnerable for conventional military threats, than for threats resulting in cyberspace. This however, is not true. In order to completely disrupt a society (thus to affect the critical infrastructure) using only military means, there really is only one option: To wage a heavy war with possible disastrous side effects. With cyber this is not the case: in the most frightening case the only thing needed would be a click on a mouse button. Cyber therefore changes the way security should be assessed.

Another important consequence for security in the cyber era may sound paradoxically. Cyber

[12] The United State even has a 'Critical Infrastructure Protection Program' identifying 14 critical infrastructures

makes it both easier and also harder to distinguish between combatants and non-combatants. This distinction between combatants and non combatants is one of the main moral guidelines during wars (Walzer, 2006). Cyber shakes up this clear-cut distinction.

On the one hand cyber van be used in a extremely discriminate way. If used properly, every single cyber action can be aimed at the one and only goal in mind. However, the opposite is also true. If discrimination is not wished for, it becomes easy to totally neglect the distinction and attack critical infrastructure. From this point of view, cyber makes thing easier.

On the other hand however, cyber extremely complicates this possibility to distinguish between combatants and non combatants. This difficulty all has to do with the following stinging question: when behind a computer, how does one know if someone is wearing a military uniform or not? Or in other words, what constitutes a combatant in cyberspace?

We can conclude this paragraph by once again underlining that as a result of the unique characteristics of cyber, looking at security is a strictly military way does not help much. Cyber threats transcend typical military threats, and have the possibility to also greatly damage critical infrastructure. An encompassing view on security could therefore be needed.

2.5.4 Hypothesis Two: the Critical Infrastructure- hypothesis

As described above the challenge in formulating an answer to how the nature of security should be assessed in the cyber era, we need to know whether it is indeed true that cyber operations have the inclination to attack critical infrastructure[13]. If this indeed is the case, this would give a good starting point for further theorizing about security in the cyber era. The second hypothesis of this thesis therefore will be as follows:

H2: If cyber war occurs, then cyber attacks will be directed at critical infrastructure

[13] If it indeed is the case that cyber war tends to be directed at critical infrastructure, this could end the distinction between combatants and non-combatants (see for example Walzer (2006).

2.6 A Core Assessment on the Future of War

Now that we have thoroughly studied the theoretical backbone of this thesis and have come up with two important, guiding hypotheses, we are able to make an assessment on how the future of war will look like in the cyber era. When thinking about the future of war it becomes interesting to try to assess the magnitude of technological developments. This thesis formulated two possible effects of cyber and will test them in the following chapters. However, this of course can never be the complete picture. Let us for a moment recall the theory of Clausewitz. According to Clausewitz 'Real Wars' are highly unlikely to evolve into 'Absolute Wars' because of the logic behind his Trinitarian model. This is a model that is completely based on a static view on international relations. The interesting question that arises is what happens if indeed our hypotheses prove states are not the leading actors anymore. Would cyber make it more likely that – in a Clausewitzian sense - 'Real Wars' evolve into 'Absolute Wars'? Of course we cannot directly test this core assessment, since no Absolute Wars have ever taken place. What we did instead is formulating two related and testable hypotheses that help us to make an assessment on the future of war and security in the cyber era. The core assessment – on which we will reflect in the concluding chapter of this thesis – is as follows

A Core Assesment on the Future of War: Challenging Clausewitz

It is more likely that 'Real War' evolves into 'Absolute War' in the cyber era than it was before cyber capabilities were present.

Now this thesis will proceed with the third chapter, which will provide us the methodological framework of this thesis.

3. Methodological Framework and Operationalization

This chapter will provide everything that is needed in order to be able to scientifically test the central hypotheses of this thesis. This means a methodological framework will be described, in which a research design is put forward. The research design will introduce the concept of case study research (and case selection strategies) as the backbone of the empirical analysis for this thesis. Furthermore attention is paid to the empirical sources this thesis relies on, as well as the justification hereof. In order to be able to indeed test the hypotheses, these hypotheses will be operationalized as is also the case with further relevant concepts.

All of this will make it possible to test the hypotheses as they were formulated in chapter two. It will moreover make it possible to test this thesis's predictions on the effects of the IT-Revolution and cyberspace on the nature of war and security. First this chapter will shortly address the research goals of this thesis. It will continue with discussing different research designs and their advantages, and will introduce the main cases that are investigated in this research project. Furthermore strategies of data collection are discussed, with this chapter wrapping up with the operationalization of the central hypotheses and concepts that are key to this thesis.

3.1 Research Goal

The central aim of this thesis is to investigate the influence of the IT-Revolution and the related coming into existence of the new domain of cyberspace on both the nature of war and the nature of security. Influential military historian Carl von Clausewitz clearly states that the nature of war is something that can never be subject to change – according to him only the nature of warfare (how wars are being fought) – can indeed change over time. This thesis seeks to critically evaluate this strong belief of Clausewitz´s. It argues that as an effect of technological innovation and development (the IT-revolution) a new domain of cyberspace has come into existence. The effects originating in cyberspace can have major impact on the nature of war[14] (for example it may be changing the likelihood of real wars evaluating into absolute wars) , and probably even challenge Clausewitz's firm belief in the unchangeable character of war. And as a result of the possible change in the nature of war, also the very nature of the concept of security might be subject to radical change as well.

[14] For a thoroughgoing analysis see chapter two.

This research project is key to the future understanding of 'what wars are', how they are fought and most importantly what their effects will be on modern societies. Technological innovations are unstoppable, and are popping up around us at an increasingly rapid pace. In order to be able to understand and investigate the wars of the future, in depth knowledge on the fundamental effects of these important developments is crucial.

3.2 Research Design: Case Study Research

This research project in general tries to investigate the effects of technological innovations in information technologies (IT) and the cyber domain on the nature of war and security. This specific research goal has the distinctive characteristic that it is studying the effects of technological phenomena that are subject to quick and constant change, pragmatism toward both the research design and the methodology is therefore needed. At first glance it is difficult to construct a satisfactory research design that is capable of testing the predictions as laid down in this thesis. This has two main reasons.

Firstly, as indicated in the foregoing introduction of this paragraph, this thesis is primarily focusing on a relatively new and rapidly changing research subject. As a consequence it is really difficult to come up with a research design that as much as possible is able to incorporate (near) future developments. This is key, since it can have profound effects on the scientific value of the conclusions of this thesis. The results of the two tested hypotheses will give us the opportunity to evaluate the broader implications of the cyber era on the nature of war and security. Moreover these two hypotheses will allow is in the conclusion to carefully interpret cyber developments in the light of Clausewitz's major idea as war unchangeable in nature[15], and subsequently provide us with tools to reflect on this idea and to come up with a core assessment on the future of war and security.

Secondly – and this is crucial as well – the domain of cyber conflict and cyber warfare has the unique characteristic of being far less 'visible' than conventional warfare. Cyber is a 'stealthy' domain, in which the outside world probably most of the times is not able to witness when a hostile attack originating in cyberspace is taking place (especially when these are minor attacks, that can be

[15] And more in specific the increased likelihood of Real Wars evolving in Absolute Wars as a result of cyber.

attributed to a lot of causes other than a cyber attack). As an effect of this, empirical cases are very scarce and so is documentation on the cases that are available. Although no direct evidence is available, it is almost certain the prevalence of cyber attacks is way bigger.

In order to overcome these two problems, a proper research design has to be constructed that as accurately as possible tackles these problems. Because the aim of this thesis is to shed light on the potential mechanisms the cyber domain creates that can change the nature of war and security, it uses a qualitative research design in this thesis, more precisely a case study research design. Where usually scholars choose for either a single case study or a multiple case study (as a sample for the complete 'population of cases'), in this research project a slightly different approach is preferred.

Instead of choosing one typical case or creating a multiple case study design, this thesis will aim to adequately map the complete 'universe' of known and reported on empirical cases in the cyber domain. Oftentimes in political science research this research design is impossible to practically work with, because of the almost infinite amount of possibly relevant cases to investigate. However, as will be showcased later in this chapter, in the cyber domain this is not the case. The cyber domain is a relatively new domain, in which well-documented cases unfortunately are still scarce. The general feeling among scholars in this specific field is that whereas many more 'incidents' and thus cases might in real occur, they are not documented for the greater public. This thesis quite logically - yet still unfortunately – only has the capability of empirically investigating cases that are known and reported on. This creates a 'universe' of relevant cases that is on the one hand feasible when it comes to its scope, and also really interesting when it comes to its scientific value. By studying practically all relevant, known cases, the conclusions of this thesis will bear both a high internal and high external validity and are therefore to be preferred over the intensive study of only one or a couple of cases.

By mapping the universe of available cases [16]and by subsequently investigating them, we will get a better view of the causal mechanisms that might be at play. The relationship between theory and empirical data can be reviewed. This creates the possibility of finding causal mechanisms and exploring how they work and what influences them (Gerring 2007, p. 90-95). In case study research it is not only the causal mechanism that is of scientific relevance. In order to get to know as much as

[16] Meaning all reported cases for which enough empirical data exists.

possible and to properly investigate any given case, every part of a presumed causal mechanism needs to be *a priori* explicated. Only when this is done, one can empirically witness *a fortiori* what the role of each variable is and if this matches the predictions of the theory. This is why the hypotheses and other relevant concepts are operationalized in paragraph 3.4 (*ibid.* p.170-173).

The main advantage of the case study research design is its high internal validity (and in this case also external validity). As a result of the in-depth study of a specific case (or group of cases), the possibility is created to test very specific and case-specific hypotheses. It has the ability to discover internal pathways. Of course case study research also has certain disadvantages.

Firstly, when it comes to validity, case study research usually strongly differs from quantitative, large-N research. The high internal validity of small-N research (case study research), inherently comes with a lower external validity (or generalizability). If however a proper research design is in place, one can minimize the negative effects on external validity so that it still is possible to generalize empirical findings. Because this thesis maps and investigates the complete universe of cases, external validity in this case will be at least as high as with large-N research and possibly even higher.

Another often heard point of critique is that when conducting case study research, it is very difficult to account for possible effect of intervening (or so-called 'third') variables that might affect variations in the dependent variable. While in large-N research one would simply include 'control variables', this is way more difficult in case study research. However, a solution to this shortcoming is indeed available. Van Evera (1997) stresses that 'when uniform background conditions are checked, the impact of possible third variables is reduced'. It is very well possible to check for these background conditions using the process-tracing method.[17] One of the advantages of this technique is that a researcher has the capability to precisely describe the mechanism but also more in depth reconstruct it. Given the complex matter of cases concerning the cyber domain, it is important to have these possibilities of getting the best and most precise picture possible before drawing final conclusions.

[17] Process tracing is a method used to reconstruct causal processes within cases. It features the use of multiple types of evidence or 'bits and pieces' (which are non-comparable) for the verification of a single outcome. In doing so it can unveil complex causal processes (George & Bennett, 2004).

3.2.1 Operationalizing the Cyber Domain: What makes a Case a Cyber Case?

As mentioned in the second chapter of this thesis on the theoretical foundations of this research project, empirical cases of cyber attacks, cyber espionage and cyber infrastructure attacks are a relatively new concept. Recalling what we concluded earlier, the cyber domain and subsequent cyber cases only came into being after the so-called Revolution in Military Affairs (RMA)[18]. For this thesis to be able to rightly distinguish between cases that relate to the cyber domain and cases that do not, an explication of the concept of the cyber domain and a description of what makes a case a 'cyber case' is needed.

When the world witnessed its first 'cyber attacks' (or phenomena that would come close to what we generally consider to be cyber attacks right now) scholars were inclined to come up with a rather restrictive definition of cyber war. According to those, cyber war was 'every instance in which a nation state engages in cyber operations' (Shakarian, Shakarian & Ruef 2013, p.21). However, with the world rapidly changing and the emergence of more relevant actors in IR than just states, the general feeling changed and asked for a more inclusive definition of the concept. The difficult question is to what extend the definition should be widened.

As Shakarian *et al.* rightly point out (*ibid.* p.21-22) it does not make sense to include – as they describe it – 'every two-bit criminal sending spam e-mails' into the definition. On the other hand one should be careful with completely excluding individuals or groups of individuals to quickly. For example terror groups like Hezbollah have already showed the world their cyber capabilities. Shakarian *et al.* dwell upon this a little further and then introduce (as was also done in this thesis before) the Clausewitzian definition of war as continuation of politics with other means. They in the end come up with the following, expanded definition, which this thesis will also use (*ibid.*p.21):

> *"Cyber war is an extension of policy by actions taken in cyber space by state or non-state actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security."*

[18] See chapter 2 for the complete analysis of the RMA

We believe the above mentioned definition best suits the current state of the cyber domain and the respective universe of cases this thesis will investigate.

It is difficult to determine when this cyber revolution in military affairs actually started and thus when the capabilities for cyber war where at levels that indeed could constitute serious threat to a state's security . Also, scholars in the field tend to disagree on this matter. The Chinese government was one of the first governments on earth to develop their own 'national cyber strategy' already in the early '90s, still a time in which a lot of people did not believe would turn out to become an important security domain. Even a decade later, in 2002 James Lewis of the Center of Strategic and International Studies (CSIS) denied the impact of the cyber domain, according to him they did not constitute a serious threat, but instead were mere 'weapons of mass annoyance' (*ibid.* p22).

Notwithstanding the critical view of Lewis and several others, views on the matter quickly changed in the years that followed. Generally the cyber actions as used by Lebanese terror group Hezbollah in the war with Israel in July 2006, are seen as the first real example of the influence of state and non-state actors in the cyber domain (*ibid.*). This thesis also takes the early 2000s as birth of the cyber domain.

3.3 Mapping the Cyber Domain Cases: Cyber Attacks, Cyber Espionage and Cyber Operations on Critical Infrastructure

As introduced in the paragraph on the research design of this thesis, in this paragraph the known and documented cases in the cyber domain will now be mapped[19]. By doing so, we will create an overview of the 'universe of cases' that will form the empirical basis that test our hypotheses with, and finally come up with conclusions.

Scholars involved in researching cyber cases have already before faced the same difficulties in creating a proper research design as this thesis does. Cases seem to be diverse and scarce, and generally seem to be 'too unknown'. In order to make the most out of the cases that in fact are

[19] Please note again that although in fact more cases have been described in certain scientific or non scientific sources, the universe of cases that is mapped in this thesis only consist of those that are well-known and documented. Other cases that as a result are not included in the indicated universe however are most likely be covered by the findings and eventual conclusions of this thesis as well.

available, some scholars have already come up with tools to adequately map the universe of cases in the cyber domain. This thesis will build on one of these approaches as introduced in the book *Introduction to Cyber-Warfare* (Shakarian, Shakarian & Ruef; 2013). These authors start their introduction into this field of research by dividing the known cases into three different subcategories (*ibid.* p.7):

1) Cyber Attacks;
2) Cyber Espionage and Exploitation;
3) Cyber Operations for Infrastructure Attack

The authors have constructed this specific distinction because of the nature of the empirical cases in each category. These categories share a 'hard core' in the fact that they are all considered to be categories covering the cyber domain, yet tiny differences are there. Because they are all slightly different, it pays off to study them as separate homogenous groups in a slightly different procedure. In doing so, the overall results will be more tangible and better conclusions can be reached that apply to cyber warfare in general.

3.3.1 Case selection

In this paragraph the empirical cases that together form the 'universe of cases' under investigation, will be introduced. All cases will be shortly discussed and will be divided into three groups hereby using the aforementioned approach. This will end up in an adequate map of all relevant and known cases.

Together these cases that are found in the scientific literature and other relevant sources, form the ideal fundament in order to be able to test the main hypotheses that are at the heart of this research project. Each of these cases provide us with a clear example of cyber activities being used by state or non state actors in order to achieve a certain political goal; in other words they showcase instances in which cyber is used as 'continuation of politics by other means'. They will hopefully provide the answers to the questions this thesis is posing.

1) <u>Cyber Attacks</u>

- **Israel-Hezbollah July War 2006**

  During the war between Israel and Hezbollah in 2006 different methods of cyber warfare were being used, most notably by the Lebanese terrorist group. Hezbollah was extremely involved in information operations, herewith trying to communicate 'their story' faster and more effectively than Israel.

- **Estonia 2007**

  On the 27th of April 2007, a series of cyber-attacks began hitting a large amount websites of Estonian organizations (for example the Estonian parliament), banks, newspapers and television broadcasters and ministries. It is generally believed these actions were related to the countries dispute with the Russian Federation over the relocation of a statue, the Bronze Soldier of Tallinn. This statue was known to be an important Soviet-era memorial and grave marker for war graves.

- **Georgia 2008**

  The war between Georgia and the Russian Federation of 2008 is the first time in history that cyber-attacks are used together with a conventional, 'shooting' war. Already weeks before the Russian military invasion of South Ossetia, hacked computers had been attacking Georgian computers and websites. It is believed that the Russians had instructed to use a broad, transnational network of computers to barrage Georgian websites, such as the ones of the parliament and of the at that time president Mikhail Saakashvilli.

2) <u>Cyber Espionage and Exploitation</u>

- **Titan Rain 2003**

  'Titan Rain' is the designation the United States gave to a coordinated series of attacks on US computer systems starting in early 2003. Although sources are not completely on one line, they have at least lasted for three years. The attacks are generally believed to be the work of the Chinese government. Main aim was to steal information from the US military industries.

- **Predator UAV- case 2009**

In 2009 US soldiers arrested a couple of insurgents in Iraq. On the laptops of these insurgents they found classified UAV footage, and the insurgents were generally believed to have obtained them via cyber capabilities. The Kata'ib Hezbollah group – which is believed to have strong links with Iran – was indicated as the main suspect.

- **US Military Contractors 2013/2014**

  In March 2014 the United States Senate Committee on Armed Services (SASC) published their investigation in which they find many 'Chinese intrusions into key defense contactors'. They found at least 20 successful intrusions in a single year, with at least another 30 that were unsuccessful.

3) Cyber Operations for Infrastructure

- **Maroochy Water Breach 2000**

  The Maroochy Water breach is a case of a cyber attack against Maroochy Water Services, a water company located in Australia. An individual hacker was able to get control over 142 water pumping stations and therewith was able to contaminate local waterways.

- **US Power Grid 2009**

  This case describes the case in which foreign hostile actors infiltrated in the US electricity grid. In doing so they were able to stealthily penetrate into this vital part of infrastructure, opening up possibilities of harming the power grid if wanted.

- **Stuxnet 2010**

  Stuxnet is the name of a computer worm that was firstly discovered in 2010/2011. It is a computer worm that is generally believed to be developed by either the Americans or the Israeli's and possibly even both. The Stuxnet worm that most probably was implanted in Iranian nuclear facilities by an undercover agent reportedly ruined almost one out of five Iranian nuclear centrifuges.

3.3.2 Strategy of Analysis

The strategy of analysis that is used in this thesis, is the 'structured, focused comparison'- approach as developed by George & Bennett (2005, p.67). These two scholars initially brought up this approach to study historical experiences in ways that 'would create generic knowledge of important foreign policy problems'. Although this thesis is not directly touching upon foreign policy and foreign policy problems, it however clearly sees the advantages of the approach of George & Bennett and therefore we think it is also useful to take it into account here as well. The main strategic aim of this approach is to study phenomena in ways that create the possibility to draw explanations of each single case under study, with the ultimate goal of putting them into a broader and more complex framework. Herewith they voice their strong reservations for using only a single case study, since generalizability there is almost impossible.

Structured, focused comparison is an approach that can be recognized by at least two important characteristics (*ibid.* p.70). Firstly, the approach is 'structured' in the way that it seeks to develop a set of standardized, general questions for each case. These questions ought to be based upon the research objective as well as the theoretical focus of the research project. The development of a set of such general questions is important because this is the only way to make sure that collection of comparable data for both cases under study is in fact possible. Secondly, the approach is 'focused' in the way that it underlines that it is paramount to have a specific research objective in mind; one that is combined with an appropriate theoretical focus. According to George & Bennett themselves (*ibid.* p.70) a researcher's treatment of a historical episode 'must be selectively focused in accordance with the type of theory that the investigator is attempting to develop.'

It is our belief that especially the first characteristic of this approach is extremely helpful for this thesis. We already often mentioned the difficulties that are involved in studying cyber cases, just to mention a few: cases are scarce, information is oftentimes lacking and maybe most importantly

cyber cases are 'stealthy'[20]. Therefore, to study them responsibly we should focus on a structured way of analysis. Standardized, general questions for each case are needed.

3.3.3 A Structured Approach: Three Important Parameters for studying Cyber Cases

In order to study the aforementioned cyber cases, this thesis now introduces its own structured approach. This approach consists of three important parameters that should be studied in each of the cases under review. Together these parameters will give a proper analysis of the specific case, and will provide us with the pieces of the puzzle we need in order to answer our overarching questions. The three parameters are as following:

1) The Main Actors involved *(needed for H1)*
    - What are the main actors involved?
    - Are they state, non-state or hybrid actors?
2) The Target and Intensity of the Operation *(needed for H3)*
    - What are the dominant means (cyber or conventional) in a specific action?
    - Was the result of the action intended or unintended?
    - Is the intensity of the specific cyber attack of the actors low, mid, or high?
    - Is the target of the attack of civilian or military nature?
3) The Capabilities of Actors involved *(needed for H1)*
    - What are the conventional military capabilities of the actors involved?
    - What are the cyber capabilities of the actors involved?

This set of standardized and general questions to be answered in each case will give us the tools we need in order to answer the questions central in this thesis. In order to indeed be able to use them, the hypotheses and other relevant concepts will now be explicated in the operationalization. Also a coding scheme is developed to use in the empirical analysis of each of the cases (see appendix).

[20] Meaning that researchers are not always able to engage in empirical research, since we just cannot 'see' anything.

3.4 Operationalization of Hypotheses and Relevant Concepts

This paragraph operationalizes the hypotheses and other relevant concepts under study. This enables us to 'measure' them, and thus to use them in the empirical study that follows in the next chapter.

Recalling the theoretical chapter of this thesis, in total two different hypotheses are formulated. Again, these two hypotheses will allow is in the conclusion of this thesis to critically evaluate and interpret the effects of developments in the cyber era and put them into a broader perspective. Especially, as laid down in the theoretical chapter of this thesis, attention will be given to the challenges these empirical results pose in the light of Clausewitz core understanding of war (and thus security) as unchangeable in nature. These results all culminate in an assessment of the future: is Absolute War more likely than before as a result of cyber capabilities?

A Core Assessment on the Future of War: Challenging Clausewitz

It is more likely that 'Real War' evolves into 'Absolute War' in the cyber era than it was before cyber capabilities were present.

- Real War

  The Clausewitzian concept of 'Real War' refers to the concept as described in the theoretical chapter of this thesis. Real War is a war situation in which rational actors [21] use violence (and thus wage war) in order to pursue their rational interests. War is a way of 'continuing politics by other means'. In this situation actors clearly live up to certain 'rules of the game'[22]

- Absolute War

  The Clausewitzian concept of 'Absolute War' refers to the concept as described in the theoretical chapter of this thesis. Absolute War is a war in which actors use massive violence (and thus wage war) in a completely unrestricted way. No rational interest are at play anymore, but instead revisionist motivations are flourishing. In this situation actors clearly deny the 'rules of the game'.

[21] For Clausewitz solely states were important.

[22] For example states after the Peace of Westphalia recognized in general each other's sovereignty

3.4.1 Hypotheses

Two separate hypotheses are derived in order to investigate the effects of cyber. Together these hypotheses – one focusing on the central actors, the other one on critical infrastructure – enable us to in the end evaluate in the effects of cyber in a broader context in IR.

3.4.2 Operationalization 'Actor'- hypothesis

The first hypothesis of this thesis is the so-called 'Actor'-hypothesis. Central in this hypothesis are the main actors that are involved in a specific cyber case. The major expectation as introduced in the theoretical chapter, namely that the power gap between state and non-state actors becomes smaller, is covered by this.

H1: When it comes to the cyber war, the differences in cyber capabilities between state and non state actors are smaller than the differences in conventional military capabilities

- Cyber War

As mentioned earlier this thesis will use the definition of Shakarian *et al.* (2013) of what constitutes cyber war: *"Cyber war is an extension of policy by actions taken in cyber space by state or non-state actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security."*

- Cyber Capabilities

Cyber capability is the ability to achieve a specified wartime objective with the use of IT and cyber technologies. In this thesis the *Cyber Power Index*[23] will be used in order to assess the cyber capabilities of states. This index rates cyber power of all states on relevant cyber components. This index does not provide information on non-state actors. Therefore non-state actors and hybrid actors

[23] Since the Cyber Power Index only investigates the G20-states, all other states will be investigated alongside the method of non-state actors.

will be assessed alongside three indicators: the number of internet connections per capita, the number of computers per capita and the school life expectancy[24]. Subsequently, in order to use these indicators, these figures will be compared to the figures of state actors on these indicators in order to benchmark the relative position of the non-state actors. Final coding will then be based upon the relative position these non state actors would have had in the *Cyber Power Index* would they only have been rated on these three indicators. It is our believe that although no ideal data is available, this will help us predict possible cyber capabilities of non state and hybrid actors.

In the analysis this variable can obtain three different scores or values (+, +/- or -). In the attached coding scheme it is thoroughly described when each of these different scores is to be registered.

- Conventional Military Capabilities

Military capability is described to be *'the ability to achieve a specified wartime objective (win a war or battle, destroy a target). It includes four major components: force structure, modernization, readiness and sustainability'* (US Department of Defense, 2014). In this thesis the conventional military capabilities of state actors will be assessed by using the *Global Firepower Index*. The conventional military power of non state and hybrid actors will be assessed by looking at the number of low intensity, middle intensity and high intensity rockets. Although this might not be an ideal measurement of the military capabilities of non state actors, it is a common method to assess the military strength of non state actors due to information shortage. In the specific case of hybrid actors we will, on top of this, look at the percentage of their GDP that is funded by external states.

In the analysis this variable can obtain three different scores or values (+, +/- or -). In the attached coding scheme it is thoroughly described when each of these different scores is to be registered.

[24] School life expectancy refers to a total number of years of schooling one can expect to receive. It is believed in this thesis that the more one is educated, the more likely it is one understands/masters cyber actions.

- State actors

A state is a nation or territory that is considered as an organized political community under one government. They enjoy both internal and external sovereignty and generally have an army to defend their interests vis-à-vis other actors. By most scholars they are seen as the most influential – if not only – actor in international relations. In the analysis this variable is scored with a (+).

- Non-State actors

Non-state actors are entities that are participate and act in the international arena and in international relations. They are different to static actors since they in no way belong to a state or its related institutions. Much discussion is concentrated not on the existence of such actors, but predominantly on their role, power and influence. In the analysis this variable is scored with a (-).

- Hybrid actors

This thesis will consider hybrid actors to be non-state actors that depend on state actors for an important part of their survival. It is chosen to make this distinction because being a hybrid actor can empower the in *de facto* non-state actor in both its military and cyber power[25]. Therefore this specific category is created. In the analysis this variable is scored with a (-).

Parameters needed to investigate this hypothesis

In order to investigate this hypothesis, two of the three aforementioned parameters (number one and three) are needed. Together these parameters, concerning the main actors involved and the military and cyber capabilities of the actors, will function as the empirical backbone of any conclusions that will be drawn on this specific hypothesis. The code schemes of the parameters will provide specific information on how to analyze each of the important components in the case studies and how to code them. Both code schemes are available in the appendix of this thesis.

[25] It is however important to note that the opposite can also be true. Hybrid actors can also be weakened by their dependence on a state actor.

3.4.3 Operationalization 'Critical Infrastructure'- hypothesis

The second hypothesis of this thesis is the so-called 'critical infrastructure'-hypothesis. Central in this hypothesis lies the theoretical assumption that cyber war tends to be directed at harming critical infrastructure, something that could – among others – indicate that Real War is more likely in the cyber era.

H2: If cyber war occurs, then cyber attacks will be directed at critical infrastructure

- Cyber War

As mentioned earlier in this chapter, this thesis will use the definition of cyber war as formulated by Shakarian *et al.* (2013, p21): *"Cyber war is an extension of policy by actions taken in cyber space by state or non-state actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security."*

- Cyber Attacks

Cyber attacks are all attacks that involve cyber capabilities

- Critical Infrastructure

Critical infrastructure are all assets (networks, systems etc.) whether physical or virtual that are vital to a community and state, so that their incapacitation or destruction would have a debilitating effect on security, economic security, national public health or safety, or any combination of it (US Department of Homeland Security). Although strictly speaking military infrastructure is also part of the critical infrastructure of a country, we will only consider civilian infrastructure to be part of this category.

Parameter needed to investigate this hypothesis

In order to investigate this hypothesis one of the three parameters is needed. In order to investigate whether cyber warfare is predominantly directed at critical infrastructure, parameter two on the target and intensity of the operation is needed. The code scheme of this parameter will provide specific

information on how to analyze each of the components relevant for this parameter. The code scheme of this parameter is available in the appendix of this thesis.

3.5 Data Collection

To be able to adequately test the hypotheses central in this research project, empirical evidence is collected from a variety of different sources. All sources that are used are relevant in their own specific way, an all have their respective advantages and downsides. In general, two big groups of sources can be divided.

Firstly, the most important source of evidence will consist of scientific contributions, such as scientific articles, books and research papers. These contributions provide empirical data and are relatively easy to check in their scientific robustness (for example via respected journals they are published in and so forth). This way we protect the objectivity of the process. Although cyber is a relatively new research subject, an increasing amount of scholars and scientific institutes and think tanks publish on the matter. Both domestically and internationally. For example the CIA and AIVD work on cyber, as well as think tanks such as Clingendael and RAND.

Secondly, this thesis will use a huge variety of non-scientific sources. Although these sources strictly viewed are not scientific per se, oftentimes the authors are respected in the field they are writing on. For example popular magazines such as *The Economist* write quite often on cyber related issues. Also, if possible this thesis will also try and approach specialists and professionals in the field.

The biggest challenge will be to attain as much information as possible on all respective cases. Sometimes this will be easy, in other instances most definitely not. We will try and put as much creativity in the process as needed, in order to succeed. Again it is important to bear in mind that pragmatism is needed also when it comes to data collection because of the nature of the field of cyber studies.

Importantly, in order to really measure the empirical date this thesis developed a coding scheme that ‘codes’ all parameters as developed in paragraph 3.3.3 (see *appendix*). This coding scheme provides a standardized method of assessing the scores in each case on every single parameter. Only by using this coding scheme we are sure that all cases under investigation will be investigated in

the same standardized way, and only when this is done we can justifiably compare the empirical outcomes of our studies. The coding scheme has tried to capture all parameters in observable and measurable ways and will be used extensively in the descriptive chapter that follows.

3.5.1 Two Important but Equally Challenging Variables

Two variables in specific are of essential importance for this research project. Unfortunately, at the same time they are really difficult to assess and measure accurately. This paragraph explicates these two essential variables, indicates the respective methodological challenges and comes up with a solution.

The first problematic variable is the 'conventional military capabilities'- variable. As laid down in the operationalization paragraph, the *Global Firepower Index* is being used to measure this specific variable. This index provides a comprehensive, quantitative tool for measuring the conventional military capabilities of a state (or Hard Power). This index however has one major downside. The most recent version of the Global Firepower Index was launched in 2014, including the most recent available data on each of the countries under analysis. Older versions of the index are nowhere available. This means that we have no exact data on the years before 2014, and thus no precise data on the years the events of our cases took place. Nevertheless, this thesis will use the Global Firepower Index of 2014 for assessing the conventional military capabilities of the state actors under investigation. This is done because of two main reasons. Firstly, the Global Firepower Index is unique in its nature. No other, comparable datasets are available that would lead to an objective assessment of the military capabilities of a country. Secondly (and most importantly), this thesis makes the assumption that the relative capabilities of all state actors under study (vis-à-vis each other) have not radically changed over the last eight years (the total time under study).

The second problematic variable is the 'cyber capabilities'- variable. As laid down in the operationalization paragraph, the *Cyber Power Index* is being used to measure this specific variable. This Cyber Power Index is the first of its kind. Never before have scholars developed such a complete and comprehensive dataset to assess the cyber capabilities of a country. In this thesis on the effect of cyber capabilities, it would be unthinkable not to use this dataset. However, this dataset has the same

major downside as the Global Firepower Index. The Cyber Power Index till today has only been launched once, in 2011. This means that no data is available from the years before and after 2011. This thesis will nevertheless still use this index two measure the cyber capabilities[26], because of two major reasons. Firstly, in the available open source data there is nothing that even comes close to the extensive dataset as provided by the Cyber Power Index, an index that is created by combining 39 indicators and sub-indicators (Cyber Power Index, 2011). It is this thesis's vast belief that to put this dataset aside and come up with a different way of measuring the cyber capabilities of states (for example the way this thesis pragmatically investigates non-state and hybrid actors) would inherently damage the robustness of the empirical findings. Secondly, when closely studying the state actors involved in this research project, we could nowhere find any evidence that would support the view that the relative differences in cyber power five years ago (2006 is the year of our first case) were decisively different than in 2011. Equally so, for the years after 2011 (in 2014 our latest case took place) we would only expect cyber capabilities to have developed even further, which wouldn't radically change our empirical analysis.

These two variables that are focusing on measuring the conventional military capabilities and the cyber capabilities, are also challenging in another way. An important part of this thesis focuses on power differences between state and non-state and hybrid actors. This means that if we want to be able to properly investigate these differences, we need to be able to measure capabilities of these different actors in a comparable way. Our method of measuring the respective capabilities of these categories of actors needs to be both valid and reliable.

In table 3.3 it is explicated how capabilities of different actors are measured. It clearly shows us that for non-state and hybrid actors, difficult decisions needed to be taken. No existing dataset was present here. For the conventional capabilities of non-state and hybrid actors, this thesis decided to look at the number and magnitude of rockets. These numbers are generally available, and give a good insight in the conventional capabilities. For the cyber capabilities of a non-state or hybrid actor, we

[26] As described before the Cyber Power Index is also used as a 'benchmark tool' for the assessment of cyber capabilities for non-state and hybrid actors. This procedure is still used, with the important remark that while the Cyber Power Index is of 2011, benchmark data of respective benchmark countries will be used from the exact years under study.

decided to look at three important variables: the number of internet connections per capita, the number of computers per capita and the school life expectancy. We believe these variables involve important enabling or disabling features for a non-state or hybrid actor to develop cyber capability. Also these specific variables are part of the sophisticated Cyber Power Index which is concerned with the cyber capabilities of state actors.

3.6 Hypotheses Confirmation and Refutation

Based on the above paragraphs, in particular the operationalization, this paragraph will conclude this chapter by determining when a specific hypothesis (and thus theory) is respectively confirmed or refuted.

Firstly, the 'Actor' –hypothesis (H1) needs to be considered falsified and thus refuted when the empirical analysis shows us that in the case of cyber war the differences in cyber capabilities between state and non state actors are not smaller than the differences in the conventional non-cyber domain. Moreover, if in a specific case a state is engaged in cyber war with a non state actor and the relative power of the non state actor vis-à-vis the state actor is comparable to that in the non cyber domain, this hypothesis should be refuted. Contrarily, if the relative power of the non-state actor vis-à-vis the state actor is indeed bigger (the non state actor scores better on cyber capabilities) this hypothesis should be confirmed.

Secondly, the 'Critical Infrastructure'-hypothesis (H2) needs to be considered falsified and thus refuted when the empirical analysis shows us that cyber attacks are not predominantly directed at critical infrastructure. This hypothesis is to be confirmed if the empirics indeed show that cyber operations mainly focus on attacking critical infrastructure.

Finally, it strongly depends on the outcomes of both hypotheses what our final assessment of the effect of cyber on the future of war and security will be. Thoroughgoing analysis and review of the results is therefore needed. If these analyses show that indeed non state actors in cyber space have gained considerable power vis-à-vis state actors, and if these analyses indeed show that critical infrastructure has become more vulnerable in the cyber era, a critical look towards an assessment of the future of war and security is needed. In case results of the two hypotheses turn out to be different, a

more thoroughgoing analysis is needed and in that case will be provided in the concluding chapter of this thesis.

Appendix Chapter 3

Parameter 1:

Table 3.1: Parameter 1

	Parameter	Explanation		Coding Definition
#1	The Main Actors involved	State Actor: only state actor	Non State Actor: only non-state actor Hybrid Actor: non-state actor(s) depending on state actor(s)	State Actors (+) Non State & Hybrid Actors (-)

Parameter 2:

Table 3.2: Parameter 2

	Parameter	Explanation	Coding Definitions
#2	The Target and Intensity of Operation		
	Dominant Means	• The dominant means being used	Cyber (+) Conventional Military (-)
	Motivation	• The motivation behind the attack	Intended (+) Unintended (+/-)
	Intensity	• The intensity of the attack	Total destruction/Revisionist: High Intensity (+) Serious violence and respective damage: Middle Intensity (+/-) Petty crimes, cyber 'bullying': Low Intensity (-)
	Target	• The target of the attack	Civilian (+) Military (-)

Parameter 3:

Table 3.3: Parameter 3

	Parameter	Explanation	Coding Definitions
#3	**The Capabilities of Actors involved**		
	State Actor	**Military** • The conventional military capabilities of a state actor • Data of *Global Firepower Index* is used	Power Index Score < 1.0 (+) Power Index Score between 1.0 and 3.0 (+/-) Power Index Score higher than 3.0 (-)
		Cyber • The cyber capabilities of a state actor • Data of *Cyber Power Index* is used for G20 countries. If not applicable method for non-state actors is being used	Cyber Power Index Score > 65.0 (+) between 30.0 and 65.0 (+/-) Lower than 30.0 (-)
	Non State Actor	**Military** • The conventional military capabilities of non-state actor • Data on number of low intensity, middle intensity and high intensity rockets	Number of high intensity rockets > middle intensity rockets (+) Number of middle intensity rockets > low intensity rockets (+/-) Number of low intensity rockets > middle intensity rockets (-)
		Cyber • The cyber capabilities of a non state actor • Data on number of internet connections per capita, number of computers per capita and school life expectancy	Numbers on variables comparable to countries in Cyber Power Index with score >65.0 (+) Numbers on variables comparable to countries Cyber Power Index with score between 30.0 and 65.0 (+/-) Numbers on variables comparable to countries Cyber Power Index with score lower than 30.0 (-)
	Hybrid Actor	**Military** • The conventional military capabilities of a hybrid actor • Data on number of low intensity, middle intensity and high intensity rockets and percentage of GDP funded by state actor.	Number of high intensity rockets > middle intensity rockets (+) Number of middle intensity rockets > low intensity rockets (+/-) Number of low intensity rockets > middle intensity rockets (-)
		Cyber • The cyber capabilities of a hybrid actor • Data on number of internet connections per capita, number of computers per capita and school life expectancy	Numbers comparable to countries in Cyber Power Index with score >65.0 (+) Numbers comparable to countries Cyber Power Index with score between 30.0 and 65.0 (+/-) Numbers comparable to countries Cyber Power Index with score lower than 30.0 (-)

4. Descriptives

This chapter will describe in detail each of the cases this thesis investigates. In total nine distinct cyber cases will be thoroughly examined. The results of this – the so called descriptives of each case - will be used to analyze and eventually test the predictions as introduced in the two hypotheses (formulated in chapter two) in the next, empirical chapter . In order to correctly describe the cases, the three parameters as brought up in chapter three are being used - together with the coding schemes - to assess the empirical data. In the end, this will lead to a descriptive foundation that is needed for the empirical analysis in the next chapter.

4.1 Empirical Analysis of Cases

This thesis will now proceed with an individual analysis of all nine cases that are under investigation. Of each of the cases a general overview will be given, after which the case will be thoroughly investigated on each of the afore formulated parameters. Each section will wrap up with a case specific conclusion.

4.1.1 Israel-Hezbollah July War 2006

Case Overview

The war between Israel and Hezbollah in July 2006 is most commonly referred to as the second Lebanon War. The second Lebanon War was a thirty-four days long military conflict mainly taking place in Lebanon, northern Israel and the Golan Heights. The war was fought between the state of Israel and the Lebanese paramilitary organization of Hezbollah. Although it is really hard to see any conflict in the Middle East out of the broader historical and regional context, the direct event that led to the outbreak of this war was the fact that Hezbollah started firing rockets at northern Israeli communities and kidnapped and later killed three soldiers. According to different sources at least 1200-1300 Lebanese people and 165 Israelis died (Economist, 2006). Also severe damage was brought to civil infrastructure (Lebanon Higher Relief Council, 2007) . Besides heavy use of conventional military means, also means of cyber warfare were part of the conflict.

Parameter 1: Actors Involved

As described in the case overview, the July War of 2006 entails the conflict between the State of Israel and Hezbollah (literally 'Party of God'), a Lebanese based Shia Islamist militant group and political party. In assessing this case alongside parameter one of our research strategy, we now have to indicate the character of the actors involved in this conflict.

It is not complicated to indicate the character of the first actor involved in this case, namely Israel. Ever since the founding of the State of Israel in 1948, Israel is a full member of the international community of states and is acting as such. Although it is easy to qualify Israel to be a state – and this thesis rightly does so – it is important to also mention the fact that Israel is not recognized to be a sovereign state by 17% of the UN member states (UN, 2014).

Deciding to qualify Hezbollah as a state, non state or hybrid actor is more complicated. Hezbollah. Initially Hezbollah was founded as a reaction to the Israeli invasion of Lebanon in 1982. Since then the organization has extended its goals and its presence in Lebanese society. The organization has grown into an organization with seats in the Lebanese government, its own media stations, social development programs, hospitals, schools and its own standing military (with fighters deployed abroad in several conflicts in the Middle East, for example in Syria). With its effective control of great parts of southern Lebanon it is often qualified to have created 'a state within a state' (Council on Foreign Relations, 2014). Although being part of the official government of the internationally recognized state of Lebanon, many states have classified Hezbollah to be a terrorist organization. Among them are the United States, the Gulf Cooperation Council and the European Union.

This thesis will however not qualify Hezbollah to effectively have the character of a state. To be a state inherently means that at least a substantive part of the international community of states recognizes an actor to be a state. No country in the world has done so. Also, more important here to note is that Hezbollah has never explicitly stated they wanted to create their own state, something that is further underlined by their presence in the current Lebanese government. This thesis however will also not qualify Hezbollah to be solely a non state actor. Hezbollah is a perfect example of a hybrid

actor.

As laid down in the operationalization of this thesis a hybrid actor is a non state actor that for its existence heavily relies on a state actor to survive. In the case of Hezbollah this undeniably is the case. With the last Israeli troops leaving southern Lebanon in 2000 (they had occupied southern Lebanon for several years) Hezbollah started to significantly increase its military capabilities. Currently it is even the case that the military capabilities of Hezbollah have surpassed the capabilities of the Lebanese Army (Barnard, 2013). This did not come out of the blue: Hezbollah heavily relies on Iran. Hezbollah receives great sums of money, military training and weapons from the Islamic Republic (Filkins, 2013). Hezbollah has effectively become an Iranian proxy in southern Lebanon. Although one might argue this situation *de facto* leads to a conflict between Israel and Iran, this is not the case in this specific context. Nowhere in the data we can find any evidence Iran has played any significant, decisive role in the outbreak of hostilities between Israel and Hezbollah in 2006. Therefore we qualify this conflict to be a conflict between Israel and Hezbollah (and not Iran).

To sum up, in this case we clearly witness a conflict between a state actor Israel (+) and a hybrid actor Hezbollah (-).

	Parameter	Explanation		Coding Definition
#1	**The Main Actors involved**	**State Actor:**	**Hybrid Actor:**	
		Israel	Hezbollah	Israel (+) Hezbollah (-)

Table 4.1: Actors Involved

Parameter 2: The Target and Intensity of the Operation

- **Dominant Means**

  The conflict between Israel and Hezbollah came to rest with UN Resolution 1701 ordering a direct ceasefire between the two fighting parties. Although both sides claimed victory, many people hold the opinion that the fact that Hezbollah was not disarmed nor destroyed points toward a victory of

Hezbollah (Inbar, 2007). This was reinforced by the war goal of Israel, that in fact was this very destruction of Hezbollah. Let us know have a closer look at what military means both sides primarily used in this conflict.

Although this case for sure has a cyber component, the dominant means being used in this conflict were of a conventional character. Both Israel and Hezbollah used heavy artillery in the conflict, in total killing thousands of people. Already during the first day of confrontation between the fighting parties, Israeli forces conducted more than a hundred attacks on southern Lebanon. During the whole conflict, the Israeli Air force flew 11.897 combat missions and the Israeli artillery and navy fired over 170.000 mortar shells (Harel and Issacharoff, 2007). Hezbollah at their side also fired back heavily. In total they fired between 3.970 and 4.228 rockets on Israel (*ibid.*).

Given these high numbers of conventional military means being used, it does not come by surprise that the dominant means in this case were not cyber related, so both Israel as well as Hezbollah score a (-) . However, cyber means were used throughout the conflict. Mainly this was done by hijacking noncombatant civilian IP addresses to help 'framing' the war effort of both sides. There were massive attempts to influence the public opinion. For example the World Union of Jewish Students created computer programs alarming people to vote in online polls and discussion forums to support the Israeli case. Hezbollah engaged in similar actions, and is believed to sometimes have been able to hack IDF station herewith obtaining intelligence (Shakarian *et al*, 2013, p34). Also Hezbollah developed a broad range of cyber propaganda mechanisms, both in Arabic and in Hebrew, especially trying to show the IDF's destruction of civilian infrastructure, herewith trying to raise support throughout the world. The UN Secretary General even quoted one of the statements that were communicated: 'No government can survive on the ruins of a nation' (UNSC Briefing, 2006)

- **Motivation**

It is not difficult to determine whether the specific actions during the 2006 war were intended or unintended. Both parties were openly at war with each other, and both wanted to reach their specific war goals. Israel wanted to destroy Hezbollah, and Hezbollah wanted to clearly stress

Israel should be aware of their power and control of southern Lebanon. Both Israel and Hezbollah score a (+). Of course the goals of both parties were different in nature, but certainly not in the motivation behind it. Both were intended. Please also note that of course it could have been the case that specific targets hit during the war were unintended (as collateral damage of miscalculations), but because the vast majority of actions were planned we will not take those into consideration.

- **Intensity**

  The intensity of the cyber actions of both sides involved in this case were of a low character (-). Generally they can be qualified as 'cyber bullying' rather than have a profound (military) effect on the outcome of the conflict. Since the mean reason behind the cyber attacks was to influence the public opinion and not so much to physically harm anything.

- **Target**

  Both parties in this war targeted both military as well as civilian infrastructure. As a direct effect of Hezbollah's used capabilities – they only used rockets to attack Israel - their actions were more indiscriminate in nature than the actions of the IDF. Hezbollah randomly fired rockets into civilian areas in northern Israel, herewith directly threatening hundreds of thousands of people living there. Hezbollah clearly scores a (+).

  The IDF on its turn is a little bit more complicated, since they attacked both military and civilian infrastructure on purpose. Although the IDF never had the goal to make as many civilian victims as possible, destroying civilian infrastructure was part of the strategy of the IDF to defeat Hezbollah in southern Lebanon. They heavily damaged civilian infrastructure, for example the Rafic Hariri International Airport in Beirut. Attacks on this civilian infrastructure has caused a lot of disapproval around the world. Since the such a large part of Israel's strategy was to cripple Hezbollah by attacking civilian infrastructure, we will also rate Israel with a (+).

	Parameter	Explanation	Coding Definitions
#2	**The Target and Intensity of Operation**		
	Dominant Means	Israel: Conventional Military Hezbollah: Conventional Military	Israel (-) Hezbollah (-)
	Motivation	Israel: Intended Hezbollah: Intended	Israel (+) Hezbollah (+)
	Intensity	Israel: Low Intensity Hezbollah: Low Intensity	Israel (-) Hezbollah (-)
	Target	Israel: Civilian Military: Civilian	Israel (+) Hezbollah (+)

Table 4.2: Target and Intensity of Operation

Parameter 3: The Capabilities of Actors Involved

- **Israel**

- Conventional

When looking at the Power Index Score, Israel scores 0.5887 (Global Firepower Index, 2014). This means Israel conventional military capabilities are rated to be high, thus scoring a (+) according to the coding scheme we developed.

- Cyber

Given the fact Israel is not a G20 country, it is not part of the Cyber Power Index. Thus it will be coded using the coding scheme of non state actors. Israel has 0.197 internet hosts per capita, a percentage of 58.25% of internet users and a school life expectancy of 16 years (CIA Factbook, 2006). Together these data make Israel score a (+) on cyber as well, since benchmark countries that score a (+) in the Cyber Power Index score accordingly on these numbers.

- **Hezbollah**

- Conventional

Although the coding procedures for hybrid actors is laid down very precisely in the coding schemes of this thesis, we however will assess the conventional military capabilities of Hezbollah in this case a little different. As already mentioned before, several authors like Barnard (2013) state that Hezbollah has surpassed the military capabilities of Lebanon. Looking at the Global Firepower Index at the score of Lebanon we see they score 2.5221 which would score Lebanon a (+/-). Given the fact that Hezbollah is seen to be stronger, they at least score a (+/-) as well. This thesis chooses to not assess the capabilities to be as extensive as needed to score a (+) since Hezbollah does not have their own navy or air force which are strong indicators Hezbollah wouldn't be able to meet themselves with the real superpowers of the world.

- Cyber

Hezbollah is a hybrid actor located in southern Lebanon. Therefore they have the possibilities of use the cyber infrastructure Lebanon provides. Lebanon only has 3307 internet hosts in total (so virtually non per capita), a percentage of 18.07% of internet users and a school life expectancy of 13 years (CIA Factbook, 2006). Together this data make Hezbollah score a (-) on cyber as since benchmark countries that score a (-) in the Cyber Power Index score accordingly on these numbers.

Table 4.3: Capabilities of Actors

	Parameter	Explanation	Coding Definitions
#3	**The Capabilities of Actors involved**		
	Israel	**Military** • Power Index Score: 0.5887	(+)
		Cyber • Internet Hosts (per capita) 0.197 • Internet Users (percentage) 58,25% • School Life Expectancy 16 years	(+)
	Hezbollah	**Military**	(+/-)
		Cyber • Internet Hosts (per capita) 0.00 • Internet Users (percentage) 18.07% • School Life Expectancy 13 years	(-)

4.1.2 Estonia 2007

Case Overview

On the 27th of April 2007 a series of cyber attacks hit several websites of Estonian organizations. These organizations included among others the Estonian Parliament, several ministries, banks and news agencies. It is generally believed that these actions were related to the country's dispute with the Russian Federation over the relocation of the statue of the Bronze Soldier of Tallinn. This statue was an important Soviet-era memorial and grave marker for war graves. Several observers of this case stressed that the level of sophistication of these cyber attacks had never been showcased before and also it is sometimes described to be the second-largest occurrence of state-sponsored cyber war (Economist, 2007). This is because almost everyone believes the Russian Federation to be, directly or indirectly, behind these attacks. As of January 2008 an ethnic Russian national of Estonia has been arrested and convicted for these attacks (BBC, 2008).

Parameter 1: Actors Involved

In this case it is not difficult at all to determine the actors that are involved in this conflict. Estonia clearly is a state actor and therefore score a (+). Although a ethnic Russian national of Estonia was arrested for the cyber attacks in this conflict, it is difficult given the evidence to deny the very strong – if not decisive – influence of Russia as the brains behind the attack. Therefore this thesis will qualify the arrested ethnic Russian not be acting on himself, but rather to be a means with which Russia conducted these cyber actions. Therefore in this case also the second actor, Russia, will be a state actor (+).

	Parameter	Explanation		Coding Definition
#1	The Main Actors involved	State Actor Estonia	State Actor Russia	Estonia (+) Russia (+)

Table 4.4: Actors Involved

Parameter 2: The Target and Intensity of the Operation

- **Dominant Means**

The dominant means as used in this case are clearly cyber means, since no conventional means were used at all in this specific conflict between Russia and Estonia. So they both score a (+)

- **Motivation**

Empirical evidence shows that the attacks as conducted clearly were intended to achieve what the achieved – being the downing of several websites and information infrastructure. As mentioned it is generally believed to be the case that Russia wanted to strongly make their voice heard in reaction to the relocation of the bronze statue. Estonia is believed to have tried to engage in cyber defensive actions that clearly were intended to defend themselves against the incoming cyber attacks. Both therefore score a (+) for intended actions.

- **Intensity**

As mentioned before the cyber attacks as allegedly ordered by Russia were of a really sophisticated character, something the world back then had not witnessed before (Economist, 2007). Also some experts qualify the difficulty of the attacks to be the ultimate proof that these actions are not something just one individual designed. According to them 'such efforts exceed the skills of individuals or of organized crime' (*ibid.*). Having said this, not everyone agrees with this characterization of Russia's cyber actions against Estonia. For example Mike Witt of the United States Computer Emergency Readiness Team (CERT) states that 'while the size of the cyber attack may be significant for the Estonian government, from a technical standpoint it is not significant in scale' (United Press International, 2007). Professor James Hendler even qualified the attacks to be 'more like a cyber riot than a military attack' (*ibid.*)

Although there are mixed opinions on the intensity of the Russian attacks, this case clearly shows the capabilities the Russian do have (but maybe not completely showcased). As middle ground Russia will therefore score (+/-). Estonia due to its mere defensive actions will score (-).

- **Target**

The target of Russia in this case clearly was of civilian nature. On purpose websites of the government, ministries, banks and media agencies were hacked to make their voiced heard. No sole military targets are known to have been attacked. Therefore Russia will score a (+).

	Parameter	Explanation	Coding Definitions
#2	**The Target and Intensity of Operation**		
	Dominant Means	Estonia: Cyber Means Russia: Cyber Mean	Estonia (+) Russia (+)
	Motivation	Estonia: Intended Russia: Intended	Estonia (+) Russia (+)
	Intensity	Estonia: Low Russia: Middle	Estonia (-) Russia (+/-)
	Target	Russia: Civilian	Russia (+)

Table 4.5: Target and Intensity of Operation

Parameter 3: The Capabilities of Actors Involved

- **Estonia**

- Conventional

  When looking at the Power Index Score, Estonia scores 3.2487 (Global Firepower Index, 2014). This means Estonia conventional military capabilities are rated to be low, thus scoring a (-) according to the coding scheme we developed.

- Cyber

  Given the fact Estonia is not a G20 country, it is not part of the Cyber Power Index (2011). Thus it will be coded using the coding scheme of non state actors. Estonia has 0.294 internet hosts per capita, a percentage of 57.75% of internet users and a school life expectancy of 17 years (CIA Factbook, 2007). Together these data make Estonia score a (+) on cyber since benchmark countries that score a (+) in the Cyber Power Index score accordingly on these numbers.

- **Russia**

- Conventional

  When looking at the Power Index Score, Russia scores 0.2355 (Global Firepower Index, 2014). This means Russia conventional military capabilities are rated to be high, thus scoring a (+) according to the coding scheme we developed.

- Cyber

  When looking at the Cyber Power Index (2011), Russia scores 31.7 meaning they have moderate cyber capacities and are coded with (+/-).

	Parameter	Explanation	Coding Definitions
#3	**The Capabilities of Actors involved**		
	Estonia	**Military** • Power Index Score: 3.2487	(-)
		Cyber • Internet Hosts (per capita) 0.294 • Internet Users (percentage) 57,75% • School Life Expectancy 16 years	(+)
	Russia	**Military** • Power Index Score: 0.2355	(+)
		Cyber • Cyber Power Index Score: 31.7	(+/-)

Table 4.6: Capabilities of Actors

4.1.3 Georgia 2008

Case Overview

During the war between Georgia and the Russian Federation of 2008 the world for the first time in history witnessed an interstate war were conventional warfare was combined with cyber warfare. Already before the Russians decided to start using heavy conventional means (with the eventual result of invading parts of Georgia) series of cyber attacks on Georgian cyber infrastructure could be

witnessed. The Russians are believed to have used a broad network of transnational based computer networks to barrage Georgian websites of among others the Parliament, the President, banks, organizations and so forth. Importantly, also news agencies were heavily attacked in order to try to influence media coverage on the conflict.

Parameter 1: Actors Involved

In this case it is not difficult at all to determine the actors that are involved in this conflict. Georgia clearly is a state actor and therefore score a (+). Russia also clearly is a state and therefore also scores a (+).

	Parameter	Explanation		Coding Definition
#1	The Main Actors involved	State Actor Georgia	State Actor Russia	Georgia (+) Russia (+)

Table 4.7: Actors Involved

Parameter 2: The Target and Intensity of the Operation

- **Dominant Means**

  The dominant means of both actors involved in this case clearly are of a conventional military character. Cyber operations were only of a supportive role during the confrontations. Both actors thus score a (-). Evidence of this can be found in the heavy conventional military means that were used – by the Russian government – to invade parts belonging to Georgia especially South Ossetia and Abkhazia. Major cities such as Gori and the capital Tbilisi have been bombed.

- **Motivation**

  Empirical evidence clearly shows that Russia acted with intend when fighting against Georgia in 2008. Again, there might have been collateral side effects that were not specifically planned for, but the overall actions were planned. This is also the case for the Georgian reaction. Both therefore score a (+).

- **Intensity**

  Let us now have a closer look at the intensity of the cyber attacks during the Russo-Georgian War. During the war Russia launched several cyber attacks that barraged and disabled many websites of South Ossetian, Georgian and Azerbaijani organizations. Also they brought down or manipulated websites of the government, ministries, news agencies and banks. For example, the website of the Georgian Parliament was hacked and replaced by images comparing president Saakashvilli of Georgia with Adolf Hitler (Wentworth, 2008). The Russians created an infrastructure in which all computers around the world could join the cyber attacks by digitally connecting their computers to a network of computers fighting Georgia. Despite these actions, several organizations were able to stop the attacks and remained working (*ibid*). Although cyber actions against Georgia are comparable to the attacks Russia conducted against Estonia, these attacks were less sophisticated in nature (probably because alongside a conventional war was going on). Therefore both Russia as well as Georgia score a (-).

- **Target**

  Again, the target of Russia in this case clearly was of civilian nature. On purpose websites of the government, ministries, banks and media agencies were hacked to support their overarching military actions. No sole military targets are known to have been attacked using cyber. Therefore Russia will score a (+).

	Parameter	Explanation	Coding Definitions	
#2	**The Target and Intensity of Operation**			
	Dominant Means	Georgia: Conventional Military Russia: Conventional Military	Georgia Russia	(-) (-)
	Motivation	Georgia: Intended Russia: Intended	Georgia Russia	(+) (+)
	Intensity	Georgia: Low Intensity Russia: Low Intensity	Georgia Russia	(-) (-)
	Target	Russia: Civilian	Russia:	(+)

Table 4.8: Target and Intensity of Operation

Parameter 3: The Capabilities of Actors Involved

- **Georgia**

- Conventional

  When looking at the Power Index Score, Georgia scores 1.7848 (Global Firepower Index, 2014). This means Estonia conventional military capabilities are rated to be average, thus scoring a (+/-) according to the coding scheme we developed.

- Cyber

  Given the fact Georgia is not a G20 country, it is not part of the Cyber Power Index. Thus it will be coded using the coding scheme of non state actors. Georgia has 0.006 internet hosts per capita, a percentage of 7.77% of internet users and a school life expectancy of 13 years (CIA Factbook, 2008). Together these data make Georgia score a (-) on cyber since benchmark countries that score a (-) in the Cyber Power Index score accordingly on these numbers.

- **Russia**

- Conventional

  When looking at the Power Index Score, Russia scores 0.2355 (Global Firepower Index, 2014). This means Russia conventional military capabilities are rated to be high, thus scoring a (+) according to the coding scheme we developed.

- Cyber

  When looking at the Cyber Power Index (Cyber Power Index, 2011), Russia scores 31.7 meaning they have moderate cyber capacities and are coded with (+/-).

	Parameter	Explanation	Coding Definitions
#3	**The Capabilities of Actors involved**		
	Georgia	**Military** • Power Index Score: 1.7848	(+/-)
		Cyber • Internet Hosts (per capita) 0.006 • Internet Users (percentage) 7.77% • School Life Expectancy 13 years	(-)
	Russia	**Military** • Power Index Score: 0.2355	(+)
		Cyber • Cyber Power Index Score: 31.7	(+/-)

Table 4.9: Capabilities of Actors

4.1.4 Titan Rain 2003

Case Overview

'Titan Rain' is the code name the United States gave to a series of coordinated attacks against US computer systems starting in early 2003. It is not completely clear for how long they have lasted, but most sources speak of 'at least three years' (Bodmer *et al*, 2012). The attacks are generally believed to be of Chinese origin. The SANS Institute – a US institute specialized in cyber security – stated that the attacks were most likely 'attempts of the Chinese military to gather information and intelligence on US systems.

Parameter 1: Actors Involved

In this case it is not difficult at all to determine the actors that are involved in this conflict. The US clearly is a state actor and therefore score a (+). China also clearly is a state and therefore also scores a (+).

	Parameter	Explanation		Coding Definition	
#1	The Main Actors involved	State Actor United States	State Actor China	United States China	(+) (+)

Table 4.10: Actors Involved

Parameter 2: The Target and Intensity of the Operation

- **Dominant Means**

  The dominant means of both actors involved in this case clearly are cyber means, since no conventional means have been used by either of the sides of this conflict (the US and China). Both actors therefore score (+).

- **Motivation**

  It is generally believed that China launched the series of cyber attacks that after that came to be known as 'Titan Rain' with the intention of gathering information on US defense systems. The US at its side did not retaliate militarily to the actions of China, but instead reacted by using cyber means to stop the Chinese attacks. Both sides thus acted with intention, and thus score a (+).

- **Intensity**

  Assessing the intensity of US cyber actions in this case is not difficult, as for as information is available only cyber counterattacks have taken place in order to stop the Chinese attacking US systems. No offensive actions are taken by the US besides these defensive acts, therefore they will score a (-) for low intensity attacks. Assessing the intensity of the Chinese attacks is more complicated. It is known that China successfully gained access to computer networks and classified information of some important US defense contractors, including Lockheed Martin, Redstone Arsenal and NASA (Bodmer *et al*, 2012). The danger in these attacks is that for a long time Chinese hackers had been able to 'be inside' highly classified systems and monitor all kinds of secret processes. The exact data the Chinese collected is not clear, but potentially the results for China were more than they had expected on beforehand. Partly because classified information of really influential organizations as NASA and Lockheed Martin had been collected, some people

speak of 'one of the biggest cyber attacks in history (SANS Institute, 2005). This thesis will rate the intensity of these Chinese attacks to be of 'middle intensity', because it clearly surpasses the qualification of 'cyber bullying' but did not have any revisionist effects on US national security. Therefore China scores (+/-)

- **Target**

The target in of this attack clearly was of military character. China tried to collect information on defense contractors possibly because they wanted to gather intelligence on US security related issues. Also one could think of economic reasons: stealing technical information on weapon systems can save one billions of dollars that usually come with the development of military material and techniques. Nevertheless, no civilian infrastructure was attacked and therefore China will score a (-).

	Parameter	Explanation	Coding Definitions	
#2	**The Target and Intensity of Operation**			
	Dominant Means	United States: Cyber Means China: Cyber Means	United States China	(+) (+)
	Motivation	United States: Intended China: Intended	United States China	(+) (+)
	Intensity	United States: Low Intensity China: Medium Intensity	United States China	(-) (+/-)
	Target	China: Military	China:	(-)

Table 4.11: Target and Intensity of Operation

Parameter 3: The Capabilities of Actors Involved

- **United States**

- Conventional

When looking at the Power Index Score, the United States scores 0.2208 (Global Firepower Index, 2014). This means the United States conventional military capabilities are rated to be high, thus scoring a (+) according to the coding scheme we developed.

- Cyber

  When looking at the Cyber Power Index, the United States scores 75.4 meaning they have high cyber capacities and are coded with (+).

- **China**

- Conventional

  When looking at the Power Index Score, China scores 0.2594 (Global Firepower Index, 2014). This means China's conventional military capabilities are rated to be high, thus scoring a (+) according to the coding scheme we developed.

- Cyber

  When looking at the Cyber Power Index (Cyber Power Index, 2011), China scores 34.6 meaning they have moderate cyber capacities and are coded with (+/-).

	Parameter	Explanation	Coding Definitions
#3	**The Capabilities of Actors involved**		
	United States	**Military** • Power Index Score: 0.2208	(+)
		Cyber • Cyber Power Index Score: 75.4	(+)
	China	**Military** • Power Index Score: 0.2594	(+)
		Cyber • Cyber Power Index Score: 34.6	(+/-)

Table 4.12: Capabilities of Actors

4.1.5 Predator UAV-case 2009

Case Overview

In 2009 US soldiers arrested a couple of insurgents in Iraq. On the laptops of these insurgents they found classified UAV footage, and the insurgents were generally believed to have obtained them via

cyber capabilities. The Kata'ib Hezbollah group – which is believed to have strong links with Iran – was indicated as the main suspect.

Parameter 1: Actors Involved

In this case it is not difficult to determine the first of the two actors involved. The first actor in this case is the United States and thus a state actor (+). The second actor is more difficult to analyze, since Kata'ib Hezbollah (not to be mixed up with the Lebanese Hezbollah party) is not extensively written about. However Shakarian *et al.* (2013, p.187) describe this group to be one of the many Shia militant groups taking part in the hostilities in Iraq. According to them these groups are heavily supported and financially funded – if not founded - by Iran. Therefore we will in this thesis consider Kata'ib Hezbollah to be an Iranian proxy and thus a hybrid actor (-).

	Parameter	Explanation		Coding Definition	
#1	The Main Actors involved	State Actor United States	Hybrid Actor Kata'ib Hezbollah	United States Kata'ib Hezbollah	(+) (-)

Table 4.13: Actors Involved

Parameter 2: The Target and Intensity of the Operation

- **Dominant Means**

  The only means used in this case are cyber means. The United States did not take any conventional or cyber military actions to respond to the hacking of the Predator UAV since they only found out about the attack afterwards when they arrested the militants and discovered the videotapes. Therefore we will only rate Kata'ib Hezbollah with a (+).

- **Motivation**

  Due to a lack of information we have no proof the hacking of the UAV was intended or not intended. We know no specific details about the goals and precise procedures that were being used by the militant group. However, since one does not easily record/steal video recordings without it being an intended action, we will rate them with a (+).

- **Intensity**

  Since the only effect of the action of Kata'ib Hezbollah was the ability to steal video recordings of the US Predator drone we cannot speak of any serious (military) threat to US interests at any time. This would have been the case if they for example would have been able to hack the control systems of the drone and for example use the weapon systems it holds. Since this all is not the case, we will qualify these actions as mere 'cyber bullying' and rate it with a (-).

- **Target**

  The target was solely military in character, thus scoring a (-).

	Parameter	Explanation	Coding Definitions	
#2	**The Target and Intensity of Operation**			
	Dominant Means	Kata'ib Hezbollah: Cyber Means	Kata'ib Hezbollah	(+)
	Motivation	Kata'ib Hezbollah: Intended	Kata'ib Hezbollah	(+)
	Intensity	Kata'ib Hezbollah: Low	Kata'ib Hezbollah	(-)
	Target	Kata'ib Hezbollah: Military	Kata'ib Hezbollah	(-)

Table 4.14: Target and Intensity of Operation

Parameter 3: The Capabilities of Actors Involved

- **United States**

- Conventional

  When looking at the Power Index Score, the United States scores 0.2208 (Global Firepower Index, 2014). This means the United States conventional military capabilities are rated to be high, thus scoring a (+) according to the coding scheme we developed.

- Cyber

  When looking at the Cyber Power Index, the United States scores 75.4 meaning they have high cyber capacities and are coded with (+).

- **Kata'ib Hezbollah**

- Conventional

Nothing is known about the conventional military capabilities of this specific militant group operating in Iraq. Most probably nothing is known about this, because they do not play any crucial role in the Iraqi conflict. Therefore we assume them to have minor military capacities, thus scoring (-).

- Cyber

Given the fact that Iraq (the country where they are fighting) is not a G20 country, it is not part of the Cyber Power Index. Thus it will be coded using the coding scheme of non state actors. Iraq has virtually no internet hosts(only 11 in total), a percentage of 1.04% of internet users and a school life expectancy of 10 years (CIA Factbook, 2009). Together these data make Iraq score a (-) on cyber since benchmark countries that score a (-) in the Cyber Power Index score accordingly on these numbers.

	Parameter	Explanation	Coding Definitions
#3	**The Capabilities of Actors involved**		
	United States	**Military** • Power Index Score: 0.2208	(+)
		Cyber • Cyber Power Index Score: 75.4	(+)
	Kata'ib Hezbollah	**Military**	(-)
		Cyber • Internet Hosts (per capita) 0.00 • Internet Users (percentage) 1.04% • School Life Expectancy 10 years	(-)

Table 4.15: Capabilities of Actors

4.1.6 US Military Contractors 2013/2014

Case Overview

In March 2014 the United States Senate Committee on Armed Services (SASC) published their investigation in which they find many 'Chinese intrusions into key defense contactors'. They found at

least 20 successful intrusions in a single year, with at least another 30 that were unsuccessful. In the report of the Senate committee 'hackers associated with the Chinese government' are specifically named to be behind the attacks. Senator Carl Levin summarized this as follows: 'These peacetime intrusions into the networks of key defense contractors are more evidence of China's aggressive actions in cyberspace' (SASC, 2014).

Parameter 1: Actors Involved

Again the actors involved are the United States (+) and China (+).

	Parameter	Explanation		Coding Definition	
#1	The Main Actors involved	State Actor United States	State Actor China	United States China	(+) (+)

Table 4.16: Actors Involved

Parameter 2: The Target and Intensity of the Operation

- **Dominant Means**

  The only means used in this case are cyber means. China only used cyber means to infiltrate in US defense systems and the United States only responded by using defensive cyber means.

- **Motivation**

  Given the fact that China already before has shown they are interested in US classified military data, it is hard to belief that this time it was not intended. Over the period of about a year, China tried at least fifty times to intrude into US classified systems, at least twenty times they succeeded to complete these actions and create a so-called *Advanced Persistent Threat* (APT). These actions can been seen to be planned beforehand and therefore score a (+)

- **Intensity**

  Although this case was made public by the Senate Committee on Armed Services itself - that at the same time also declassified a great part of their final research report – it is still not easy to assess the relative intensity of these attacks as compared to the attacks against the US that China

conducted in the past. The lion's share of the report speaks about how to counter these attacks in the future, and not so much on the impact past attacks have had on US interests. Most probably this was done because of security related motivations. Since nothing indicates these attacks are of greater intensity than during 'Titan Rain' it will also rate these attacks to be of middle range intensity. Therefore also these will score (+/-)

- **Target**

  The target of these attacks as conducted by China are highly comparable to the ones that were observed during operation 'Titan Rain'. They are strictly military in nature, most probably both from a security as well as an economic interest. Therefore China scores a (-) for military targets.

	Parameter	Explanation	Coding Definitions	
#2	**The Target and Intensity of Operation**			
	Dominant Means	United States: Cyber Means China: Cyber Means	United States China	(+) (+)
	Motivation	United States: Intended China: Intended	United States China	(+) (+)
	Intensity	United States: Low Intensity China: Medium Intensity	United States China	(-) (+/-)
	Target	China: Military	China:	(-)

Table 4.17: Target and Intensity of Operation

Parameter 3: The Capabilities of Actors Involved

Since in this case again the two actors are the same as in the case of 'Titan Rain', we will not again describe the military and cyber capabilities of both China and the United States, but will just copy the overview as was constructed already.

	Parameter	Explanation	Coding Definitions
#3	**The Capabilities of Actors involved**		
	United States	**Military** • Power Index Score: 0.2208	(+)
		Cyber • Cyber Power Index Score: 75.4	(+)
	China	**Military** • Power Index Score: 0.2594	(+)
		Cyber • Cyber Power Index Score: 34.6	(+/-)

Table 4.18: Capabilities of Actors

4.1.7 Maroochy Water Breach 2000

Case Overview

The Maroochy Water breach is a case of a cyber attack against Maroochy Water Services, a water company located in Australia. An individual hacker was able to get control over 142 water pumping stations and therewith was able to contaminate local waterways.

Parameter 1: Actors Involved

In this case the first actor, Australia clearly is a state actor (+). The individual held responsible for the hacking of the water company is a non state actor (-).

	Parameter	Explanation		Coding Definition
#1	**The Main Actors involved**	**State Actor** Australia	**Non State Actor** Individual	Australia (+) Individual (-)

Table 4.19: Actors Involved

Parameter 2: The Target and Intensity of the Operation

- **Dominant Means**

  In this case only the individual, later named to be Vitek Boden (a former contractor working for the company), was using cyber means in order to achieve his goals. Neither Australia defense forces nor the company tried to defend itself by using cyber or military actions. The individual hacker will therefore score a (+).

- **Motivation**

  In the judicial hearings of Vitek Boden after he got arrested for his actions, he pledged he attacked the Maroochy water company because they did not hire him for a job he wanted to have (Shakarian *et al.*, 2013, p.206). Clearly, he intended to do what he did. The score therefore will be (+).

- **Intensity**

  As a direct result of the actions of the hacker, he got control of 142 water pumps. He did this by only using a laptop and a radio transmitter. During his attack he released more than one million liters of contaminated and untreated sewage water into a storm water drain that flowed into local waterways (*ibid.*). It is likely to have affected many people living in the region that for their freshwater relied on the company. The intensity of this attack is not to be underestimated. Although it might look like a frustrated individual taking revenge at his former employer, the effects of this were substantial and potentially could have been way worse. Imagine he for example would have contaminated the water not only by untreated sewage water, but instead would have inserted toxic materials as well. Because of the fact he directly affected many people living in the vicinity of the company, we rate this attack to be of a middle range character and therefore to score it with a (+/-).

- **Target**

  The target that was attacked in this case is of civilian nature. It goes without saying that water supplying companies are part of the critical infrastructure of a country. Therefore the score will be (+).

	Parameter	Explanation	Coding Definitions
#2	**The Target and Intensity of Operation**		
	Dominant Means	Individual: Cyber Means	Individual (+)
	Motivation	Individual: Intended	Individual (+)
	Intensity	Individual: Medium Intensity	Individual (+/-)
	Target	Individual: Civilian	Individual: (+)

Table 4.20: Target and Intensity of Operation

Parameter 3: The Capabilities of Actors Involved

- **Australia**

- Conventional

When looking at the Power Index Score, Australia scores 0.8253 (Global Firepower Index, 2014). This means Australia's conventional military capabilities are rated to be high, thus scoring a (+) according to the coding scheme we developed.

- Cyber

When looking at the Cyber Power Index (Cyber Power Index, 2011), the United States scores 71.0 meaning they have high cyber capacities and are coded with (+).

- **Individual**

- Conventional

The individual has no conventional military means available, therefore he scores a (-).

- Cyber

Given the fact that the hacker operated in Australia, the score of Australia as scored in the Cyber Power Index will also be applicable for the individual here. The hacker scores a (+).

	Parameter	Explanation	Coding Definitions
#3	**The Capabilities of Actors involved**		
	Australia	**Military** • Power Index Score: 0.8253	(+)
		Cyber • Cyber Power Index Score: 71.0	(+)
	Individual	**Military** None	(-)
		Cyber • Cyber Power Index Score: 71.0	(+)

Table 4.21: Capabilities of Actors

4.1.8 US Power Grid 2009

Case Overview

This case describes the case in which foreign hostile actors infiltrated in the US electricity grid. In doing so they were able to stealthily penetrate into this vital part of infrastructure, opening up possibilities of harming the power grid if wanted in the future. Although they did not do that at the very moment of infiltrating the systems, officials warned that at the moment they were 'mapping the infrastructure' which they could use in case they in fact wanted to do harm.

Parameter 1: Actors Involved

Again the actors that are involved are the United States and allegedly predominantly Chinese hackers. Both are state actor, scoring (+).

	Parameter	Explanation		Coding Definition
#1	**The Main Actors involved**	**State Actor** United States	**State Actor** China	United States (+) China (+)

Table 4.22: Actors Involved

Parameter 2: The Target and Intensity of the Operation

Since the means and motivation of this series of Chinese attacks again is highly comparable to both Titan Rain and the case of the military contractors, we will not again describe all three components of this parameter, since they are almost all alike. Only the target in this case clearly is civilian (+), because the actions were specifically aimed at the civilian power grid.

	Parameter	Explanation	Coding Definitions	
#2	**The Target and Intensity of Operation**			
	Dominant Means	United States: Cyber Means China: Cyber Means	United States China	(+) (+)
	Motivation	United States: Intended China: Intended	United States China	(+) (+)
	Intensity	United States: Low Intensity China: Medium Intensity	United States China	(-) (+/-)
	Target	China: Civilian	China	(+)

Table 4.23: Target and Intensity of Operation

Parameter 3: The Capabilities of Actors Involved

Since in this case again the two actors are the same as in the case of 'Titan Rain', we will not again describe the military and cyber capabilities of both China and the United States, but will just copy the overview as was constructed already.

	Parameter	Explanation	Coding Definitions
#3	**The Capabilities of Actors involved**		
	United States	**Military** • Power Index Score: 0.2208	(+)
		Cyber • Cyber Power Index Score: 75.4	(+)
	China	**Military** • Power Index Score: 0.2594	(+)
		Cyber • Cyber Power Index Score: 34.6	(+/-)

Table 4.24: Capabilities of Actors

4.1.9 Stuxnet 2010

Case Overview

Stuxnet is the name of a computer worm that was firstly discovered in 2010/2011. It is a computer worm that is generally believed to be developed by either the Americans or the Israeli's and possibly even both. The Stuxnet worm that most probably was implanted in Iranian nuclear facilities by an undercover agent reportedly ruined almost every one out of five Iranian nuclear centrifuges.

Parameter 1: Actors Involved

In this case potentially three actors are involved. All of these are state actors, namely the United States (+), Israel (+) and Iran (+).

	Parameter	Explanation		Coding Definition
#1	The Main Actors involved	State Actors United States Israel	State Actor Iran	United States (+) Israel (+) Iran (+)

Table 4.25: Actors Involved

Parameter 2: The Target and Intensity of the Operation

- **Dominant Means**

  In this case no conventional military means were used by any of the actors. Only Israel and the United States are believed to have used cyber means (+) to develop the Stuxnet-worm. Most probably they used an undercover special agent to – via USB-stick – make the virus infiltrate into the Iranian nuclear facilities.

- **Motivation**

  The action by the United States and Israel can be perceived to be fully intended. Both countries throughout the last decades, since the Islamic Revolution, have openly voiced their fear of Iran using nuclear facilities not for peaceful means but to develop a nuclear bomb. Therefore this action can be seen as intended (+).

- **Intensity**

  The Stuxnet virus is generally perceived to be really successful in achieving the main aims it was constructed for. Nearly one out of every five nuclear centrifuges in the attacked nuclear facilities have been completely destroyed (*ibid.* p 323). The intensity of the attack therefore is of a considerable intensity. This thesis scores the intensity of this attack to be of middle intensity (+/-), since the effects were not revisionist in character. Instead of destroying the complete facilities indiscriminately, the attacked was discriminate and only focused on limited aims. Therefore it scores (+/-)

- **Target**

  This thesis will qualify the target to be military in nature (-). Of course one could also make the case that attacking nuclear infrastructure that is being used for the peaceful means of creating power for civilians is part of a countries critical infrastructure and therefore civilian in nature. However, because the intention of the attack was not to shut down power supplies (but instead destroy centrifuges that are not needed for the peaceful use of nuclear facilities) we will nevertheless code these attacks to be aimed at military targets.

	Parameter	Explanation	Coding Definitions
#2	**The Target and Intensity of Operation**		
	Dominant Means	USA & Israel: Cyber	(+)
	Motivation	USA & Israel: Intended	(+)
	Intensity	USA & Israel: Medium Intensity	(+/-)
	Target	USA & Israel: Military	(-)

Table 4.26: Target and Intensity of Operation

Parameter 3: The Capabilities of Actors Involved

- **United States**

- Conventional

When looking at the Power Index Score, the United States scores 0.2208 (Global Firepower Index, 2014). This means the United States conventional military capabilities are rated to be high, thus scoring a (+) according to the coding scheme we developed.

- Cyber

When looking at the Cyber Power Index, the United States scores 75.4 meaning they have high cyber capacities and are coded with (+).

- **Israel**

- Conventional

When looking at the Power Index Score, Israel scores 0.5887 (Global Firepower Index, 2014). This means Israel conventional military capabilities are rated to be high, thus scoring a (+) according to the coding scheme we developed.

- Cyber

Given the fact Israel is not a G20 country, it is not part of the Cyber Power Index. Thus it will be coded using the coding scheme of non state actors. Israel has 0.23 internet hosts per capita, a percentage of 61.53% of internet users and a school life expectancy of 16 years (CIA Factbook, 2010). Together these data make Israel score a (+) on cyber as well since benchmark countries that score a (+) in the Cyber Power Index score accordingly on these numbers.

- **Iran**

- Conventional

When looking at the Power Index Score, Iran scores 0.8891 (Global Firepower Index, 2014). This means Iran's conventional military capabilities are rated to be high, thus scoring a (+) according to the coding scheme we developed.

- Cyber

Given the fact Iran is not a G20 country, it is not part of the Cyber Power Index. Thus it will be coded using the coding scheme of non state actors. Iran has 0.002 internet hosts per capita, a percentage of 10.68% of internet users and a school life expectancy of 15 years (CIA

Factbook, 2010). Together these data make Iran score a (-) on cyber as well since benchmark countries that score a (-) in the Cyber Power Index score accordingly on these numbers.

	Parameter	Explanation	Coding Definitions
#3	**The Capabilities of Actors involved**		
	United States	**Military** • Power Index Score: 0.2208	(+)
		Cyber • Cyber Power Index Score: 75.4	(+)
	Israel	**Military** • Power Index Score: 0.5887	(+)
		Cyber • Internet Hosts (per capita) 0.23 • Internet Users (percentage) 61.53% • School Life Expectancy 16 years	(+)
	Iran	**Military** • Power Index Score: 0.8891	(+)
		Cyber • Internet Hosts (per capita) 0.002 • Internet Users (percentage) 10.68% • School Life Expectancy 15 years	(-)

Table 4.27: Capabilities of Actors

This chapter has provided this thesis with the descriptive foundation that is needed in order to investigate and analyze the empirical data in a structured way. The next chapter will take this descriptive foundation as a starting point for the empirical analysis and subsequent hypotheses testing.

5. Analysis

In this chapter the two earlier formulated hypotheses central to this thesis will be tested to investigate the effect of increasing cyber capabilities and cyber warfare on the nature of war and security. At this point again it is important to recall the pragmatic case selection strategy this thesis chose: instead of investigating one or two cases, this thesis decided to map and investigate the complete universe of cases that are reported upon. This can have consequences on the outcome of the analysis for specific hypotheses[27].

The first hypothesis that is tested in this chapter is the 'Actor'-hypothesis. This hypothesis predicts a smaller difference in capabilities between state actors and non state actors when it comes to cyber domain as opposed to the differences in the 'conventional' military domain. The expectation is that non state actors – when compared to state actors – are relatively stronger in the cyber domain.

The second hypothesis that is tested in the chapter is the 'Critical Infrastructure'-hypothesis. This hypothesis predicts that cyber capacities create a higher degree of vulnerability for critical infrastructure than conventional military capacities. Moreover is predicts that cyber attacks are predominantly focusing on harming critical infrastructure.

After thorough investigation of these two hypotheses and their results, this thesis in the concluding chapter will try to make a core assessment on the future of war and security as already formulated in chapter two and three. It will challenge the fundamental beliefs of Clausewitz on the unchangeable character of the nature of war.

5.1 Analysis of the Actor-hypothesis

In order to analyze whether the power balance between state and non-state actors in the cyber domain is different that the power balance in the conventional military domain we will now first return to the hypothesis we derived in chapter two.

H1: When it comes to the cyber war, the differences in cyber capabilities between state and non state actors are smaller than the differences in conventional military capabilities

[27] For example this effect can be clearly seen when analyzing hypothesis one (the Actor-hypothesis) where in fact only three out of the in total nine cases are suitable for investigation (the other six are state-state cases).

The above mentioned hypothesis (H1) was derived from the theoretical assumption – as explained in chapter two – that for non state actors it is easier and extremely less expensive to acquire cyber capabilities than to acquire conventional military capabilities.

In order to investigate this specific hypothesis, two parameters as constructed in chapter three are needed. It concerns the 'main actors involved'- parameter and the 'capabilities of actors involved'-parameter. In the descriptive chapter each of the nine cases under study were coded on these two parameters.

5.1.1 Analysis of the Main Actors Involved (Parameter 1)

When having a closer look at the first parameter, we observe something interesting. Out of the nine cases that together form the 'universe of cases' this thesis has mapped, only three cases show a conflict between state actor on the one hand and a non state or hybrid actor on the other hand. This means that two-thirds (and thus the vast majority) of the known and reported upon cyber cases describe a conflict between two state actors.

Let us know have a closer look at the three cases in which a non state or hybrid actor was present. Again something interesting appears. Out of the three cases, we can see that only in the 'Maroochy Water Breach 2000' case a non state actor is engaging in offensive cyber operations. In the two other cases – 'Israel-Hezbollah 2006' and 'Predator UAV 2009' – we witness hybrid actors to be engaging in offensive cyber operations. Although the descriptives for both of these cases do not indicate any direct involvement of the sponsoring state of the hybrid actors (notably Iran in both cases) in the specific cyber operation, we can clearly see that in cyberspace non state actors acting completely independent are a scarce phenomenon[28].

We tend to observe that offensive cyber operations - at least insofar we can assess – are primarily 'state business' and are primarily being used as an asset in inter-state conflict. Besides the fact that sovereign states extensively use cyber operations themselves, it also seems that sovereign

[28] Of course oftentimes it is reported that international gangs and organized crime are involved in cyber operations in order to steal (personal) information or money. Therefore one should bear in mind the possibility that non-state actors are omnipresent in cyberspace as well, but not – at least till today – thoroughly reported upon.

states tend to sponsor cyber operations of hybrid actors across the globe to serve their specific (regional) interests. In doing so, they can pursue their respective interests without having to openly interfere themselves.

It seems to be relatively easy and cheap – and thus attractive and functional – to sponsor the buildup of cyber capacities of hybrid actors[29]. Once a state actor has built up cyber capabilities at one of its proxies (the hybrid actors), these capacities can function as a offensive cyber 'stealth capacity' ready to be used when needed. Building up a comparable conventional capacity is oftentimes more difficult, because of the visibility of these actions and the vigilance of other actors.

5.1.2 Analysis of the Capabilities of Actors Involved (Parameter 3)

Because of the fact that hypothesis one (H1) is primarily concerned with the relative power differences in the cyber domain between state and non-state or hybrid actors, this paragraph will first examine the three cases – as indicated above – in which state actors in fact were in conflict with non-state or hybrid actors. After the analysis of these three specific cases, we will shortly come back to the other six cases and the relative power differences between state actors in the cyber domain. Parameter 3 would support hypothesis one (H1) if indeed the expectation is true that power differences between non state/hybrid actors and state actors are smaller in the cyber domain than in the conventional domain.

When analyzing the results of this parameter, it is important to recall the research methodology behind the measurement of both the conventional and cyber capabilities of the actors. Because cyber is a relatively new, rapidly evolving and technologically challenging area of research it is difficult to come up with a sound way of measuring data. Pragmatism therefore is needed[30].

Let us now first have a look at the 'Israel-Hezbollah 2006' case. Conventionally Israel is stronger than Hezbollah (+ vs. +/-). We would expect the capability difference in the cyber domain to be smaller. However this is not the case. Israel scores a (+) and Hezbollah scores a (-). The difference in capabilities in the cyber domain in this case is even bigger than in the conventional domain.

In the 'Predator UAV-case 2009' we see a comparable picture. In the conventional domain the

[29] In the cases under study, we can clearly see Iran to be involved in these actions
[30] For an extensive explanation and justification of chosen methods see chapter three

US scores a (+) and Kata'ib Hezbollah a (-), similarly in the cyber domain the US also scores a (+) and Kata'ib Hezbollah also a (-).

An opposite picture arises when analyzing the third case, the 'Maroochy Water Breach 2000'. While there is an enormous unbalance in the conventional domain between Australia (+) and the individual (-), this unbalance is almost completely gone in the cyber domain where both actors score a (+).[31] It would be interesting to analyze why this case shows a different picture than the two aforementioned cases in which it clearly seemed not to be the case that the power difference between non state/hybrid actors and state actors in the cyber domain is relatively smaller than in the conventional domain.

The most striking observation that can be made is the fact that the two first cases in which cyber capabilities were not highly developed (the Israel-Hezbollah and the UAV case), are cases that are both attached to the same geographical region (the Middle East). This triggers theorizing about the possibility that in both cases actors were constrained by the technological environment in which they had to operate. The Middle East in general and Lebanon and Iraq in specific[32] are technologically (meaning when it comes to IT-infrastructure and 'cyber') not highly developed. It could very well be possible that due to these technological constraints both actors did not have the capacity to develop their cyber capabilities. On top of this, also the general level of education in these countries tend to be relatively low, with Lebanon having an average of 13 years of education and Iraq only 10. Also this can have a profound impact on the IT-related knowledge that is necessary to develop sophisticated cyber capabilities. This could lead to educational constraints.

Australia in contrast, is highly technologically developed and has an extensive education system. The technological and educational constraints as seen in Lebanon and Iraq are not applicable here, contrarily so one could say the IT-environment and the level of education in Australia can be seen as key enablers for cyber development and capabilities. This could be (part of) the explanation of the differences between the cases.

[31] It is important to underline that although both countries score a (+) this however still does not mean they are equally strong. Part of this inaccuracy is caused by the method of measuring the cyber capabilities of non-state actors, where not all data can be incorporated (as is done in the Cyber Power Index) – for example the effect of manpower.

[32] The only exception to this might be the case of Israel

Following this line of reasoning we would also expect to find similar patterns when it comes to the cyber capabilities of state actors under investigation. If indeed technological and educational constraints matter, these should also affect state actors. This indeed seems to be the case. From the state actors under investigation only four countries – Australia, Israel, United States and Estonia - score the maximum score of (+). China and Russia score a (+/-) and Georgia is the only country to score a (-). When having a closer look at the data, it indeed is the case that the higher a country scores on cyber capabilities, the lesser the constraints are applicable (and thus the developed educational and technological environment works as an enabler for the development of cyber capabilities) .

5.1.3 Conclusion Actor-hypothesis

Based on the analysis of the data as presented above, it becomes possible to determine whether the expectation as laid down in hypothesis one (H1) can be confirmed or needs to be refuted.

When analyzing the data it becomes clear that with regard to the expectation that the power difference in the cyber domain between state and non state/hybrid actors is smaller than in the conventional domain, is difficult to defend. Out of the three cases under investigation, this turned out to be the case only once. In two out of the three cases, we were not able to empirically showcase the effect as expected in the hypothesis. Consequentially, we need to reject hypothesis one. There is no evidence non state/hybrid actors are relatively stronger in the cyber domain than in the conventional domain. No evidence is found for Van Creveld's 'dying state' hypothesis.

Although we cannot do anything different at this time than refuting hypothesis one, we need to bear in mind an important caveat as described in the analysis. Only one of the three cases investigated took place in a technologically and educationally highly developed region, and this specific case seems to support hypothesis one. This raises the important additional questions.

5.2 Analysis of the Critical Infrastructure-hypothesis

In order to analyze whether critical infrastructure is indeed more vulnerable in cyber warfare than in conventional warfare, we will now first return to the hypothesis we derived in chapter two.

H2: Critical infrastructure is more vulnerable for cyber threats than for conventional military threats

The above mentioned hypothesis (H2) was derived from the theoretical assumption – as explained in chapter two – that cyber operations (as opposed to conventional operations) are more likely to aim at harming critical infrastructure. Almost all of contemporary critical infrastructure relies on IT and is therefore more vulnerable for attacks specifically using these technologies.

In order to investigate this specific hypothesis, one parameter as constructed in chapter three is needed. It concerns the 'Target and Intensity of Operation'- parameter. In the descriptive chapter each of the nine cases under study were coded on this parameter.

5.2.1 Analysis of the Target and Intensity of Operation (Parameter 2)

Because of the fact that hypothesis two (H2) is primarily concerned with the vulnerability of critical infrastructure in cyber warfare, this paragraph will at first thoroughly examine the outcomes of the descriptives on parameter two[33] on the 'dominant means' used in the conflict and the 'target of the cyber operation'. Together these two parts of parameter two will give us the empirical evidence we need in order to confirm or refute hypothesis two. The two other parts of this parameter – the motivation and the intensity of the attacks – will provide us with more background information to further underpin our findings. Parameter two would support hypothesis two (H2) if indeed the expectation is true that critical infrastructure is more prone to be attacked in cyber operations than in conventional operations.

Out of the nine cases under investigation, only in two cases the dominant means of warfare are conventional in nature (in case three and nine). This means that in all other six cases the dominant means of warfare are completely or predominantly cyber related. Of course, one might argue this is not a surprising finding, since cases in this thesis are selected because of their cyber nature. This is only partly true. It is true that this thesis selected cases because of the presence of cyber operations in the specific described conflict. However what is not true is that we only looked out for and selected

[33] A complete overview on the outcomes of parameter two is given in the appendix of this chapter.

cases in which cyber necessarily was dominant. Instead, we were only interested in cases in which the cyber means were adequately described and reported upon, no matter whether cyber in that case was dominant or not. This means we can at least say something about this specific distribution.

Out of the documented nine cases only in two cases cyber means were used as part of a more integrated and comprehensive military strategy in which conventional and cyber means are combined. In six cases cyber operations were not used in addition to conventional means, but used solely on their own instead. This is an interesting finding, since it is quite regularly argued that cyber operations are more and more becoming part of integrated military strategy in the future (Pentagon, 2014).

Let us now have a look at the specific targets of the military operations as described in our nine cases. Our data shows that operations in five cases were specifically aimed at harming civilian infrastructure and four cases aimed at harming military infrastructure. It is interesting to see that in both cases in which conventional means were dominant – the Israel/Hezbollah case and the Georgia case – the targets were civilian in nature. Contrarily, only in three out of the seven cases in which cyber means were dominant, actions were specifically aimed at civilian infrastructure.

In order not to draw conclusions on these characteristics too quickly, we need to know more about the specific cases in which cyber means were used to attack military infrastructure. This is important because of course the reasoning behind the classification of the targets of the operations is a methodological one.

In three out of the four cases in which cyber means were used to attack military targets (Titan Rain, the Predator-UAV and Military Contractors case), cyber means were used to infiltrate military IT-infrastructure in order to steal classified information. These actions were strictly non-kinetic in character. In the fourth case – Stuxnet – cyber means were used to infiltrate Iranian nuclear facilities and kinetically do harm. Let us first recall how this thesis operationalized the concept of critical infrastructure:

Critical infrastructure are all assets (networks, systems etc.) whether physical or virtual that are vital to a community and state, so that their incapacitation or destruction would have a debilitating effect

on security, economic security, national public health or safety, or any combination of it. (Chapter three, p.57)

Also the crucial decision was made to exclude military infrastructure from the definition of critical infrastructure:

Although strictly speaking military infrastructure is also part of the critical infrastructure of a country, ***we will only consider civilian infrastructure to be part of this category.***

If we critically evaluate this decision to exclude military infrastructure from the definition, the outcomes of our descriptives (and subsequently the judgment on this hypothesis) would look radically different.

Looking back at the specific cases we would be able to include two of the four aforementioned cases under 'critical infrastructure'. This would change the numbers into a situation in which seven out of the nine cases were aimed specifically at critical infrastructure, with five out of seven cyber cases specifically aiming at harming critical infrastructure. And in fact there is a strong case to make to include the 'Titan Rain' and 'Military Contractors' cases in the critical infrastructure definition. Both cases are describing deep penetrations into classified IT-infrastructure of the US military, resulting in many successful instances of theft of valuable economic and security related information. Given the magnitude and nature of these actions, we could argue these two cases are an example of assets that are 'vital to a state [The US]' and that endanger the economic and military security of the United States. Especially because in both of the cases the invader was China, the country that is challenging the US for world-leadership. Therefore we decide to – in retrospect – include these two cases under the critical infrastructure definition.

It is not completely clear why in fact it is the case that critical infrastructure is more vulnerable to cyber operations that to conventional operations. Although we did not find any direct evidence, it could very well be the case that the 'stealthy' characteristics of cyber are important here as well. When cyber is used to attack critical infrastructure, it is really difficult to clearly witness the operations and the effects of operations. Recall the situation of the Maroochy Water Breach. In this situation – among

other things – a water company was shut down because of offensive cyber actions. From the outside these actions however were not visible. For the public the company could very well be facing a technical problem, instead of being attacked. Now try to imagine this same company to be attacked conventionally, for example someone drops a bomb on it. Now everyone would clearly see the company was attacked. Most likely this would generate a completely different outcome. This could be part of the explanation why cyber is so often used to attack critical infrastructure.

What is also interesting to see is that in none of the investigated cases results of the respective operations were unintended. In all nine cases outcomes of operations are described that were intended.

When looking at the intensity of the operations in our cases, we clearly see that in none of the nine cases high intensity operations were executed. This means that none of the operations sought to change the status quo. Six out of the seven cyber cases at least had components of middle intensity operations in them, with many of the cyber cases showcasing both middle intensity and low intensity cyber operations. When further analyzing these cases, we see that offensive cyber actions in our cases were all the times of a middle intensity character. The reacting defensive cyber actions were always low intensity, countering operations.

5.2.2 Conclusion Critical Infrastructure-hypothesis

Based on the analysis of the data as presented above, it becomes possible to determine whether the expectation as laid down in hypothesis two (H2) can be confirmed or needs to be refuted.

When analyzing the data it becomes clear that the expectation that cyber attacks tend to be directed at critical infrastructure is supported by the empirics. Therefore hypothesis two should be confirmed. Out of the in total nine cases, in seven cases cyber means were specifically aimed at harming critical infrastructure (although they were only the dominant means in five of these seven cases). In only two cases this was not the case.

This empirical data clearly shows us that cyber capabilities have often been used to specifically target critical infrastructure, something that has been described more often in the scientific literature (for example Ericcson 2010, Erikson and Giacomello 2006). Hypothesis two needs to be confirmed.

5.3 Additional Finding: Cyber as a Framing Mechanism

Apart from the main findings of this thesis concerning the hypothesis, this thesis also found another interesting additional finding that eventually can be used for further research.

It is interesting to see that in three of the nine cases, offensive and defensive cyber operations were used especially to influence public opinion by 'framing' a specific conflict or specific actions. Here cyber capabilities were used to try and change opinions and mobilize support. These actions were aimed at people that are directly involved in the conflict as well as people that have no direct connections to a conflict (or 'the rest of the world'). We see that in both cases in which conventional military means were dominant, cyber means were used to frame the conflict. During the Israel-Hezbollah war of 2006, both sides of the conflict extensively used the internet to influence the opinions and views of the conflict all around the world. Aggressive internet campaigns were used to achieve these goals. These campaigns were not only started or sponsored from the parties directly involved in the conflict, it also turns out that cyber makes it easier for supporters of a specific cause (for example the Jewish Diaspora in this case) to actively take part in a conflict. Similar patterns occurred during the Estonian and Georgian case. In both instances the Russian government used cyber operations to frame the conflict, generally by verbally and non-verbally referring to a feeling of Russian nationalism.

5.4 General Results and Conclusion

In this chapter the Actor -hypothesis (H1) and the Critical Infrastructure –hypothesis (H2) were tested. In paragraph 5.1 the assumption was tested that in the cyber domain the differences in capabilities between state and non-state actors are smaller than in the conventional domain. No empirical evidence was founded to support this assumption. Hypothesis one had to be rejected. In paragraph 5.2 the assumption was tested that critical infrastructure is more vulnerable for cyber operations than for conventional operations. This thesis found convincing evidence that this indeed is the case. Therefore hypothesis two was confirmed. Also we found empirical data that might indicate that cyber capabilities are more often being used as a framing mechanism. This is an area for further research.

In the next concluding chapter of this thesis these results will be taken into account when we try to come up with the core assessment on the future of war. We try to answer the overarching question of this research project, by critically evaluating whether innovations in the cyber domain create a need to change our contemporary views on the nature of war and security.

Appendix Chapter 5

Table 5.1: Parameter Overview.

	Parameter Overview			
#2	**The Target and Intensity of Operation**			
	Dominant Means	**Cyber** Case #: 2,4,5,6,7,8,9		**Conventional** Case #: 1,3
	Motivation	**Intended** All cases		**Unintended** No cases
	Intensity	**High** No cases	**Middle** Case #: 2,4,6,7,8,9	**Low** Case #: 1,2,3,4,5,6,8
	Target	**Civilian** Case #: 1,2,3,7,8		**Military** Case #: 4,5,6,9

Note: in the 'intensity' category some case numbers appear twice. This is because in these cases two separate cyber actions were witnessed. In most cases this entailed an offensive cyber action and a defensive cyber action as a reaction. For the exact explanation for each case, please see the description of the specific case.

6. Conclusion and Remarks

This sixth and final chapter of this thesis consists of a critical reflection on the research project and the empirical results. It reflects on the implications of the methodological decisions that were made. Concluding this chapter we come up with the final, overall conclusions of this research project. We will do so by formulating an answer to the central research question as it was introduced in the introductory chapter. In the end this will lead to a core assessment on the future of war and security in the cyber era.

6.1 The Cyber Revolution and the Nature of War and Security

The first chapter of this thesis started off by introducing the most recent *Global Threat Assessment* (2013) of the Director of National Intelligence (DNI) of the United States. This report provided an analyses of the most prevalent threats to the national security of the United States. In 2013, for the first time in history threats originating in cyberspace were topping this list. According to the report the 'importance and reach [of cyber threats] as a global threat cannot be overstated' (*ibid.* p2).

In recent decades major technological developments have taken place, predominantly in the area of information technologies (IT). These developments together led to the birth of cyberspace; a new and completely digitalized domain. The 21st century is the century of digitalization. This technological revolution can be witnessed throughout our societies: it can be seen when we buy something online or when we swipe our credit card. This birth of cyberspace is also the birth of a new domain of potential conflict: cyber conflict.

The coming into existence of cyberspace turned out to be potentially problematic for current theories of International Relations. All theories in IR – for example realism - are modeled along certain specific assumptions on the nature of war and related nature of security. This means that if cyber developments change this assumed nature of war and security – and there are reasons to believe they do - these theories would face serious problems. This led us to the following research question:

To what extent and in what way does the cyber revolution change the nature of war and security in the 21st century?

6.2 Theorizing the Effects of Cyber: Actors and Targets in Cyberspace

In order to investigate this overarching research question central to this thesis we first developed a theoretical framework to map the current state of the theoretical debates and indicate the gaps in the scientific literature. In doing so, we were able to come up with two testable hypotheses that enabled us to investigate theoretical assumptions that underpin the research question more thoroughly

The theoretical chapter started off with the foundations on nature of war theory as formulated by Carl von Clausewitz. One of the main assumptions as developed by Clausewitz is that war is a continuation of policy/politics of a state by other means, and it is a strictly unchangeable concept. Where methods of war (or warfare) might change, the nature of war never does. Based on this state centric world view, Clausewitz develops a model in which he explains the rationale behind wars and comes up with his logic why 'Real Wars' almost never evolve into 'Absolute War' – his Trinitarian model.

The theoretical chapter continues by questioning what would happen in the case of a breakdown of the general foundational assumptions of this Trinitarian theory. It raises the question what would happen to his logic behind absolute wars if cyber developments would cause the breakdown of the state centric paradigm. Would in the cyber era for example the concept of friction still be able to stop a negative spiral toward absolute war; or would absolute war become more likely?

One of the main theoretical schools challenging the Clausewitz's views on the unchangeable nature of war is brought together by scholars investigating the Revolution in Military Affairs (RMA). One of their main points is that as an effect of technological developments, both the methods of war as well as the nature of war are subject to change. This thesis takes the RMA as a starting point and starts theorizing how developments in the cyber domain could influence the nature of war and eventually the nature of security[34]. It herewith strongly focuses on views of Choucri (2012) and Van Creveld (2004) and subsequently comes up with two hypotheses. The two hypotheses concentrate on the relevant actors in cyberspace and their respective capabilities (H1) and on the targets of cyber operations (H2).

[34] This thesis makes the assumption that – as explained in chapter two – the nature of war and the nature of security are interconnected concepts.

These two hypotheses form the basis for a core assessment on the future of war and security in the cyber era: is Absolute War more likely?

Because of the difficult nature of research on developments in the cyber domain, pragmatism was needed in the whole process. Although this thesis initially aimed to empirically test this core assessment, this turned out to be impossible. Instead, the aforementioned two separate and testable hypotheses were formulated.

As one can see, both hypotheses concentrate on situations of (cyber) war and conflict. This issue is most pressing in hypothesis one. Hypothesis one expects that when it comes to cyber war, differences in cyber capabilities between state and non state actors are smaller than the differences in the conventional military domain. This does not mean these power differences are not present when war or conflict is absent. This thesis however decided to formulate the hypothesis as it was done, because the power differences only become salient in times of war and conflict.

6.3 Results and Findings

The descriptive and empirical chapter together served to provide a solid basis so that both hypotheses could be tested. The first hypothesis to be tested (H1) was as follows:

> **H1:** When it comes to the cyber war, the differences in cyber capabilities between state and non state actors are smaller than the differences in conventional military capabilities

For each of the nine selected cases of the universe of cases that we mapped we investigated if the actors involved in the specific conflict were state or non state/hybrid actors. Subsequently we coded their conventional military capabilities as well as cyber capabilities. The expectation was that the differences in cyber capabilities between state and non state/hybrid actors are smaller than the differences in conventional military capabilities. This assumption turned out not to hold. Based on the empirical evidence that was provided, hypothesis one needed to be rejected.

The second hypothesis (H2) that was tested in this thesis was as follows:

> **H2:** If cyber war occurs, then cyber attacks will be directed at critical infrastructure

For each of the nine selected cases of the universe of cases that we mapped we investigated if the actors involved in the specific conflict specifically aimed their cyber attacks at military targets or civilian critical infrastructure. The theoretical expectation was that in cyber operations civilian critical infrastructure would more likely be targeted than military targets. This assumption turned out to hold. Based on the empirical evidence that was provided, hypothesis two needed to be confirmed.

These findings make it possible to answer the central research question of this thesis. As the empirical analysis shows us, the presence of the cyber domain and cyber capabilities has an effect on the nature of war and security in the 21st century.

Our first hypothesis shows us that contrarily to what is oftentimes stated, until now cyber capabilities have not significantly impacted the powerful position of states in the international arena. It is not the case that non state or hybrid actors have greatly strengthened their position and are now in the position to seriously challenge the primacy of states. Nevertheless, it is difficult to draw the bold conclusion that because of this, the nature of war has not changed at all as an effect of cyber. Proponents of Clausewitz would state that the nature of war hasn't changed as a result of cyber. Clausewitz's main theoretical building block is still in place: the state. This means his Trinitarian model is still applicable and the nature of war thus still unchangeable. Opponents of Clausewitzian theory such as Mary Kaldor would possibly name cyber developments to again be a sign the nature of war is really changing.

This thesis holds a middle ground position. The empirics show us that whether cyber changed the nature of war or not, cyber developments are closely followed and taken into account. The fact that cyber threats top the *Global Threat Assessment* is a strong signal: if cyber does not change the nature of war, it certainly changes our conception of war and conflict in the future.

Our second hypothesis shows us that the nature of security is subject to change as an effect of cyber capabilities. Our results show that cyber attacks are almost always directed at critical infrastructure. This means that we can expect that if cyber warfare increases in the future – which is likely – critical infrastructure will be targeted more often. Where conventions of wars in the past created a situation in which critical infrastructure was oftentimes spared – and thus the distinction

between combatants and non-combatants protected – cyber wars lay these conventions aside. This changes the nature of security.

6.4 Theoretical and Methodological Considerations

Concluding this thesis it is always useful to reflect on the theoretical and methodological choices that were made throughout the process of writing this thesis. These decisions guided the empirical research, and can have profound effects on its findings. This is especially the case in this specific research project, since cyber is a difficult to investigate due to its nature.

The most important decisions we had to take at the very beginning of the theoretical chapter of this thesis was that it turned out to be impossible to directly test the core research question of this thesis on the increasing likelihood of absolute wars in the cyber era. Instead we derived relevant hypotheses that at least could provide us with part of the answer.

One of the first important decisions that needed to be made in the methodological chapter was the exact definition of what constitutes a cyber case. We needed to find the right balance in which cases to include and which cases explicitly not to include. As we formulated it in chapter three we did not want to include 'every two-bit criminal sending spam e-mails'. The solution that was formulated provided a definition in which only cases of cyber warfare were selected that pose 'a serious threat' or are conducted in response to a perceived threat against a nation's security. This definition led to the nine cases we investigated.

In hindsight this decision might have caused some serious consequences. For example in our findings we conclude that cyber operations are – contrarily to what we might have expected – predominantly state business. The prevalence of non state and hybrid actors was less than expected. This might very well have been different had we expanded the definition of cyber cases we used. Had we done so then for example many cases of major cyber theft and criminality would have been part of our project. This might have influenced our findings concerning hypothesis one and possibly also concerning hypothesis two.

Furthermore due to difficulties in finding useful data, we had to develop our own coding mechanism in order to investigate the hypotheses. In chapter three, three parameters were described

and coding schemes were introduced to measure the relevant empirical data. This thesis put a lot of effort in creating a method that serves both a high reliability and high validity, but very well realizes this is difficult to achieve. Empirical findings and conclusions drawn upon are influenced by the methodological framework we developed, and might have looked different had we used a different methodology.

Let us for example have a look at the way this thesis assesses the conventional military capabilities and cyber capabilities of actors involved. As described in chapter three, we had to make pragmatic choices to find the data needed for a proper assessment on these capabilities. Especially in the case of the measurement of cyber capabilities of non state and hybrid actors – which is crucial to this thesis – we had to think out of the box. Data was scarce and not always reliable. We decided to look at certain enabling/disabling conditions that might indicate cyber power, such as levels of connectivity and levels of education. Although the data that was used is accurate, of course different data could have led to different outcomes and potentially different conclusions in this thesis.

Already in the empirical chapter we critically reflected upon some methodological decisions that were made especially in the operationalization of some of the concepts relevant in this thesis. For example we pointed toward the conceptualization of 'critical infrastructure'. The definition we worked with initially excluded military critical infrastructure, something that significantly influenced our initial findings. Sometimes we had to rethink the reliability of some of the concepts.

It is important to also reflect on the core assumptions that underpin our theoretical line of reasoning in chapter two. In this chapter current theories of International Relations in general - and realism more in specific - are judged to be unable to explain international relations in the cyber era. Of course these views would not easily be accepted by most scholars belonging to those specific schools of theory. Instead of accepting the need for completely new theories to be developed, they more likely would rather point toward starting points for incorporating cyber developments into their own theories[35]. Although this might by partly or completely true, for this thesis it is not relevant to try and counter all these specific claims. Instead what this thesis does is developing a theoretical line of reasoning that would lead to a general revision in the way we look at IR and the assumptions that

[35] See for example the article by Erikson and Giacomello (2006)

underpin this. In the end this might lead to views that can either be incorporated in current theories or might create a starting point for new theories to be developed.

When it comes to evaluating the data we used to base our empirical findings on, what we can clearly see is that almost all sources originate in the United States and Europe. This is interesting, especially since our findings in several of the cases showcase solely non-Western countries (Russia and China) to be aggressors in cyberspace. It is hard to believe that only non-Western countries would conduct offensive cyber operations, which underlines the necessity to critically look at least part of the empirical data. Unfortunately sources outside the Western world are usually not available in English, which made it impossible to incorporate them in this project.

6.5 Scientific Progression and Areas for Future Research

The research project as conducted in this thesis tried to explore a relatively new field in debates in international relations. The study of cyber space and cyber conflict is relatively new; radical technological developments of the recent past boosted the importance of this relatively new area of research. As described, the year 2013 was the first time cyber threats were recognized to be taken seriously. With technology increasing by the day, we expect cyber studies to gain more importance rapidly. It is our steadfast belief we are at the brink of an era of cyber conflict.

Because of the pioneering character of the thesis, one in general should see this project to be one of the first attempts to come up with an assessment on how the world might look like in the cyber era. It is one of the first attempts to map the history of known cyber conflicts and to investigate some of the core claims that are being made on cyber conflicts in general. This thesis serves as a profound basis for future research on how cyber shapes future conflict.

Based on the empirical findings of this thesis, we would like to give some specific recommendations for future research. An important area of research would be to investigate how geographical differences influence the current balance of cyber power. In this thesis we found evidence that major differences in cyber capabilities exist between ‘developed’ countries and less developed countries across the globe. Probably they are – at least partly – causes by technological and educational constraints. With technology rapidly spreading across the globe, it lies within expectation

that these difference become smaller in the foreseeable future. Also it is important to realize that the current unbalance in technological possibilities possibly works two ways: technologically developed countries have greater capabilities to conduct cyber operations, but are also more vulnerable.

We would also greatly applaud any efforts to develop mechanisms to more in thorough measure cyber capabilities of state and non state actors. With better tools to access this information we would immediately be able to draw bolder conclusions. Possible directions for research lie within trying to come up with more quantifiable indicators that demonstrate cyber capabilities (this thesis came up with educational and technological indicators).

Lastly and important lesson can be found in the realization that cyber is a slippery and stealthy concept. Most of what is happening probably takes place without us seeing or even realizing it. Therefore the expectation is that when it comes to cyber conflict, way more is going on than we can actually described in this thesis. In depth case studies on known cases can help understanding the multidimensional and sophisticated rationale behind cyber operations. This eventually will help us to map the cyber domain better. In this respect also the 'framing' motivations behind cyber operations as found in chapter five can be further investigated.

6.6 A Core Assessment on the Future of War and Security

In this last paragraph of this thesis we will try to answer the overarching research question of this thesis, or in other words we will try to come up with a core assessment on the future of war and security in the 21st century. The era of cyber conflict. As explained in the introductory chapter we brought up a general research question on how the nature of war and security might change as a result of developments in the cyber era. In the theoretical chapter that followed we specified this research question, postulated two hypotheses and tried to reflect on the basic views of Clausewitz that are at the basis of many of our contemporary views on war and security. Our core assessment was formulated as follows:

> It is more likely that 'Real War' evolves into 'Absolute War' in the cyber era than it was before cyber capabilities were present.

The two hypotheses that were tested in this thesis are part of our ability to assess whether the above mentioned assessment comes close to reality. Unfortunately even at the end of this research project we are still unable to come up with a definite answer.

Based on the empirics we can boldly state that the technological developments of the recent past have a great magnitude and will almost for sure be of major impact in conflicts in the future. Conflicts of the future will be influenced by the cyber domain, and will incorporate cyber operations. The main question is to what extend: will cyber operations ever take the position conventional capabilities hold right now? Or will cyber capabilities always be supportive of leading conventional operations? We think this is completely dependent on future technological developments, but it could very well be the case that cyber becomes more dominant and maybe even leading. Part of our findings in this thesis explain just why.

As we were able to see when we investigated the first hypothesis on the empowerment of non state and hybrid actors in the cyber domain, until now it is not the case that the relative position of non state and hybrid actors has significantly improved as an effect of cyber. This means that Van Creveld's (2004) 'dying state' thesis does not hold. Our results of the second hypothesis show us that cyber attacks – as opposed to conventional attacks - tend to be directed critical infrastructure. What does this mean in terms of the core assessment on the future of war and security? `

The fact that states are not challenged by non state actors as a result of cyber, means that we can expect that Clausewitz's Trinitarian model still holds in the cyber era. We did not find any evidence that in the cyber era there are factors that would challenge the rationale behind this theory. Moreover, we expect the state to function similarly in the cyber domain as in the conventional domain. This would indicate there is no reason to think Absolute Wars in the cyber era are more likely.

However, it is interesting to question the influence of cyber on the important concept of friction – the controlling mechanism that prevents wars to evolve into absolute wars. As we saw in the theoretical chapter, friction can be seen as everything that makes war in practice different than on paper. For example one could think of weather condition or poor logistics. Due to rapid technological developments we are able to increase our control of daily life. Conditions that were out of our control in the past, can nowadays be controlled using technology. We are using computers to more closely

register inventories and to make logistical plans. Sometimes we are even able to control the weather[36]. With technologies increasing, this may indicate friction can disappear in the future. This would challenge the Trinitarian model.

The fact that cyber attacks predominantly focus on critical infrastructure is also interesting in the light of the likelihood of absolute wars to occur. If in the future indeed critical infrastructure is attacked and destroyed more often, it is likely that this will have an effect on the impact of war and conflict on societies. Clausewitz states that absolute wars are not likely, because of friction and because of the absence of popular backing for an all out war. Where friction might be disappearing as an result of technology, the popular aversion of absolute war might disappear as an effect of critical infrastructure being targeted in cyber war. If cyber war destroys all vital infrastructure for a society to work, then what is relevance for fighting a war with restricted aims: absolute war might very well be the only way out.

Even though cyber is relatively new we were already able to bring up cases in which individuals or groups of people penetrate into critical infrastructure. Especially the UAV and Maroochy Water Breach case give us an example on how this might work. In these two cases the effects and scope of the actions were limited, but the same actions and technologies could also be used for similar, but way more unrestricted actions. If one can penetrate into the operating system of a drone, why would it be impossible to penetrate into the operation system of a commercial airliner or warplane?

In sum, it is difficult to predict what will happen in the future. Technology is increasing fast, and so are the effects of it on societies. In our hypotheses we did not find unanimous support for the assessment that absolute wars are more likely in the future. What we did come up with is a comprehensive picture of how cyber developments until now have influenced the nature of war and security.

We do not think Absolute War as Clausewitz describes will be happening already tomorrow because of these developments. It could even be the case that in the next decades the influence of cyber is 'contained' by strong barriers of conventional capabilities. As a result, current theories of

[36] See for example China using silver iodide to control rain.

international relations might still be relevant for decades to come. However as our relatively new and pioneering project clearly shows, it will just be a matter of time. Technology has changed mankind itself and equally so it will change the way mankind wages war. Eventually the nature of war and security will change.

List of References

Alker, H. R. (1988). The dialectical logic of Thucydides' melian dialogue. *American Political Science Review*, 82(3), 805-820.

Art, R. J., & Jervis, R. (2008). *International Politics: Enduring Concepts And Contemporary Issues*. New Jersey, NJ: Pearson.

Baldwin, D. A. (1997). The concept of security. *Review of international studies*, 23(1), 5-26.

Barnard, A. (2013). *Developments in Syria*. Retrieved November 18, 2014, from http://www.nytimes.com/2013/05/21/world/middleeast/syriadevelopments.html?pagewanted=all&_r=1&

Bendrath, R. (2001). The cyberwar debate: Perception and politics in US critical infrastructure protection. *Information & Security: An International Journal*, 7(1), 80-103.

Bodmer, S., Kilger, M., Carpenter, G., & Jones, J. (2012). *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. New York, NY: McGraw Hill Professional.

Booth, K. (1991). Security and emancipation. *Review of International studies*, 17(4), 313-326.

Buzan, B. (2000). The Logic of Regional Security in the Post-Cold War World. In *The New Regionalism and the Future of Security and Development*, edited by Bjorn Hettne, Andras Inotai and Aswaldo Sunkel. New York, NY: St. Martin's Press

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers.

Campen, A. D., Dearth, D. H., & Goodden, R. T. (1996). *Cyberwar: Security, Strategy and Conflict in the Information Age*. Fairfax: AFCEA International Press.

Choucri, N. (2012). *New Challenges to International Relations Theory and Policy*. Cambridge, MA: MIT Press.

Clapper, J.R. (2013). *Worldwide Threat Assessment to the House Permanent Select Committee on Intelligence.* Retrieved November 18, 2014, from https://www.hsdl.org/?search&collection=public&fct&so=score&submitted=Search&offset=0&page=1&tabsection=Congressional+and+Legislative+Resources&creator=Clapper%2C+James+R.+(James+Robert)%2C+1941-.

Clausewitz, C. Von (2004). *On war*. New York, NY: Barnes & Noble Books.

Cordesman, A. H. (2002). *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the US Homeland*. Westport: Praeger.

Council on Foreign Affairs. (2014). *Renewed Conflict in Syria*. Retrieved November 18, 2014, from http://www.cfr.org/lebanon/renewed-conflict-lebanon/p33083.

Cyber Power Index (2011). *Findings and Methodology*. Retrieved November 18, 2014, from http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf.

Ericsson, G. N. (2010). Cyber security and power system communication—essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery*, 25(3), 1501-1507.

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) relevant theory? *International Political Science Review*, *27*(3), 221-244.

Factbook, C. I. A. (2006, 2007, 2008, 2009, 2010). *The World Factbook*. Retrieved November 18, 2014, from https://www. cia.gov/library/publications/the-world-factbook.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23-40.

Fierke, K. M. (2007). *Critical Approaches to International Security*. Cambridge, MA: Polity Press.

Filkins, D. (2013). *The Shadow Commander*. Retrieved November 18, 2014, from http://www.newyorker.com/magazine/2013/09/30/the-shadowcommander?currentPage=all

Freedman, L. (2013). *The Transformation of Strategic Affairs* (No. 379). London: Routledge.

George, A. L., & Bennett, A. (2005). Case Studies and Theory Development in the Social Sciences. Cambridge, MA: MIT Press.

Gerring, J. (2007). Case study research. Principles and Practices. Cambridge, MA: MIT Press.

Global Firepower Index (2014). *Global Firepower Index 2014.* Retrieved November 18, 2014, from http://www.globalfirepower.com/

Global Threat Assessment (2013). *Global Threat Assessment 2013*. Retrieved November 18, 2014, from http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf

Goodman, W. (2010). Cyber Deterrence. Tougher in Theory than in Practice? *Strategic Studies Quarterly*, 4(3), 102-135.

Gray, C. S. (2010). War—Continuity in Change, and Change in Continuity. *Parameters*, 40(1), 5-13.

Green, L. (2002). *Communication, Technology and Society*. London: Sage Publication Ltd.

Harel, A., & Issacharoff, A. (2007). *34 days: Israel, Hezbollah, and the War in Lebanon*. Basingstoke: Palgrave Macmillan.

Holmes, J.R. *Everything you know about Clausewitz is wrong.* Retrieved November 20, 2014, from http://thediplomat.com/2014/11/everything-you-know-about-clausewitz-is-wrong/

Inbar, E. (2007). How Israel Bungled the Second Lebanon War. *Middle East Quarterly*, 20(4), 57-65.

Jervis, R. (1979). Deterrence Theory Revisited. *World Politics*, *31* (2), 289-324.

Kagan, F. W. (2003). War and Aftermath. *Policy Review*, 120(3), 3-27.

Kaldor, M. (2013). *New and Old Wars: Organised Violence in a Global Era*. Stanford, CA: Stanford University Press.

Katzenstein, P. J. (Ed.). (1996). *The Culture of National Security: Norms and identity in world politics*. New York, NY: Columbia University Press.

Keegan, J. (2004). *A History of Warfare*. New York, NY: Random House.

Keohane, R. O., & Nye Jr, J. S. (1998). Power and Interdependence in the Information Age. *Foreign Affairs*, 77(5), 81-94.

Langner, R., & Pederson, P. (2013). *Bound to Fail: Why Cyber Security Risks Cannot Simply Be "Managed" Away. Cyber Security Series*. Washington, DC: Brookings.

Lebanon Higher Relief Council. (2007). Retrieved November 18, 2014, from http://fr.jpost.com/servlet/Satellite?cid=1167467714626&pagename=JPost%2FJPArticle%2FPrinter

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica: Rand Corporation.

Lin, H. S. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy*, 4(1), 63-86.

Lippmann, W. (1944). *US War Aims*. Boston: Little, Brown.

Lupovici, A. (2010). The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda. *International Studies Quarterly*, *54*(3), 705-732.

Lupovici, A. (2011). Cyber Warfare and Deterrence: Trends and Challenges in Research. *Military and Strategic Affairs, 3(3),* 49-62.

Nayak, M., & Selbin, E. (2010). *Decentering International Relations*. London: Zed Books.

O'Hanlon, M. E. (2002). A Flawed Masterpiece. *Foreign Affairs*, 81(3), 47-63.

Owen, T. (2004). Human security-conflict, critique and consensus: Colloquium remarks and a proposal for a threshold-based definition. *Security Dialogue*, 35(3), 373-387.

Rajkumar, R. R., Lee, I., Sha, L., & Stankovic, J. (2010*). Cyber-Physical Systems: The Next Computing Revolution*. In Proceedings of the 47th Design Automation Conference 2010, 731-736. Retrieved November 18, 2014, from http://dl.acm.org/citation.cfm?id=1837274

Rogers, C. J. (1995). *The Military Revolution Debate: Readings on the Military Transformation of early modern Europe*. Boulder, CO: Westview Pr.

Rousseau, D. L., & Garcia-Retamero, R. (2007). Identity, Power, and Threat Perception A Cross-National Experimental Study. *Journal of Conflict Resolution*, 51(5), 744-771.

SANS Institute. (2005). *Cyber Guardian*. Retrieved November 18, 2014, from http://www.sans.org/cyber-guardian

SASC. (2014). *Press Release on Chinese Intrusions.* Retrieved November 18, 2014, from http://www.armed-services.senate.gov/press-releases/sasc-investigation-finds-chinese-intrusions-into-key-defense-contractors.

Schelling, T. C. (2008). *Arms and Influence: With a New Preface and Afterword*. New Haven, CT: Yale University Press.

Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Waltham, MA: Syngress.

Singer, P. W. (2011). *Corporate warriors: The Rise of the Privatized Military Industry*. Ithaca, NY: Cornell University Press.

The Economist (2006). *Hizbullah's new offensive.* Retrieved November 18, 2014, from http://www.economist.com/node/7912789

The Economist (2007). *A cyber-riot.* Retrieved November 18, 2014, from http://www.economist.com/node/9163598

Ullman, R. H. (1983). Redefining security. *International security*, 8(1), 129-153.

United Nations (2014). *Recognition of Israel*. Retrieved November 18, 2014, from http://www.jewishvirtuallibrary.org/jsource/Peace/recogIsrael.html

United Nations Security Council Briefing. (2006). Retrieved November 18, 2014, from https://www.google.nl/search?q=Harel+Issacharoff&hl=nl&gws_rd=ssl#hl=nl&q=unsc briefing 2006 no government can survive on the ruins of a nation%e2%80%99

United Press International (2007). *Analysis who cyber smacked Estonia*. Retrieved November 18, 2014, from http://www.upi.com/Business_News/Security- Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/UPI-26831181580439/

US Department of Defense (2014). *US Doctrine*. Retrieved November 18, 2014, from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Van Creveld, M. (2004). The Fate of the State. In *The State of Europe: Transformations of Statehood from a European Perspective*, 33-50, edited by Puntscher, S., Mokre, M., & Latzer, M. New York, NY: Campus Verlag

Van Creveld, M. (2009). *Transformation of War*. New York, NY: Simon and Schuster.

Van Creveld, M. (2010). *Technology and war: From 2000 BC to the present*. New York, NY: Simon and Schuster.

Van Evera, S. (1997). *Guide to methods for students of political science*. Ithaca, NY: Cornell University Press.

Walt, S. M. (1991). The Renaissance of Security Studies. *International Studies Quarterly*, 35(2), 211-239.

Walzer, M. (2006). *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. New York, NY: Basic Books.

Watts, B. D. (2004). *Clausewitzian Friction and Future War*, McNair Paper 68. Washington, DC: National Defense University.

Wentworth, T. (2008). *You've Got Malice: Russian Nationalists Waged a Cyber War against Georgia. Fighting Back Is Virtually Impossible*. Retrieved November 18, 2014, from http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111

Wolfers, A. (1962). *Discord and Collaboration: Essays on International Politics.* Baltimore: The Johns Hopkins Press.