

# Cyber warfare

Connecting classical security theory to a new security domain

Gabriel  
Strinde

# Abstract

This paper examines how cyber warfare as a new empirical phenomenon can be understood and explained through the classical security theory of realism. As states begin to view cyberspace as part of their strategic interest, the main divisions of neorealism provide different explanations as to the intentions and interactions of states. The hypothesis of this paper is that realism is not enough to understand or explain the new empirical phenomenon of cyber warfare on its own. I conclude the paper by examining the strengths and weaknesses of realism core features, specific arguments provided by the main division within neorealism as well as arguing the main asymmetry to the concept of power produced by the introduction of cyber warfare into the security theory.

*Keywords:* cyber warfare, realism, state, internet, power, military capabilities

Characters: 61 708

# Table of contents

<b>1</b>	<b>Introduction.....</b>	<b>1</b>
1.1	Research question.....	2
1.2	Purpose of the paper.....	2
1.3	Method.....	3
1.3.1	Material and previous research.....	4
<b>2</b>	<b>Theoretical framework.....</b>	<b>5</b>
2.1	Classical realism.....	7
2.2	Neorealism.....	8
2.2.1	Waltz's neorealism.....	8
2.2.2	Offensive realism.....	10
2.2.3	Defensive realism.....	11
<b>3</b>	<b>Cyber warfare.....</b>	<b>14</b>
3.1	Understanding cyber warfare.....	14
3.2	Confronting cyber warfare.....	19
<b>4</b>	<b>Analysis.....</b>	<b>22</b>
4.1	Cyber war and Waltz's neorealism.....	25
4.2	Cyber war and offensive realism.....	27
4.3	Cyber war and defensive realism.....	29
<b>5</b>	<b>Conclusion.....</b>	<b>32</b>
<b>6</b>	<b>References.....</b>	<b>34</b>

# 1 Introduction

The internet has since its beginning revolutionized the way our society works. Especially in the West, a large portion of our society is directly connected through the internet which has made it possible to order food directly to your door without leaving your house, purchase tickets for international travel or check your mail on your phone on the way to work. Many states also rely on the internet for their civilian and military infrastructure as well as coordination between various parts of the military. Such a dependency on the internet has produced a new security problem for many states that now view cyberspace as part of their strategic interest.

Cyber war is a new phenomenon that has not been fully revealed yet. Richard A. Clarke and Robert K. Knake have defined cyber war as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption".<sup>1</sup>

Though much is still not revealed about cyber warfare, there are events considered to be the starting point of cyber warfare between states as the effect of them and level of sophistication has all but ruled out the involvement of any actor but a state with advanced technological capacity. These events in connection with continuous reports of aggressive cyber activity between states should prove enough that cyber warfare, if not fully revealed, still is considered by many states to be a new and functional battleground.<sup>2</sup>

I will in this paper explain how cyber warfare can be understood and why many states regard it as a strategic interest. With the focus on states the natural choice of theory for this paper is realism that I will use to examine how the

---

<sup>1</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 6

<sup>2</sup> Masters, Jonathan, *Confronting the cyber threat*, Council on foreign relations, 2011, retrieved 26 April 2011, <<http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577>>

dominant classical security theory views state actions and how cyber warfare can be understood from it as well as the effect of cyber warfare on realism.

I got the idea for this paper in a hotel room in Moscow after watching a late night documentary on cyber warfare from BBC, the only English speaking channel on the hotel. Though portraying cyber warfare a bit like the new nuclear weapons of our time I found the subject to be interesting as it was largely unknown to me and I had not seen much discussion on it within peace and conflict studies.

## 1.1 Research question

With cyber warfare being a fairly new addition to the strategic interests of states I found it interesting to examine the impact classical security theory and cyber warfare would have on each other. As such, my research questions are *how can cyber warfare be understood through classical security theory?* and *how does cyber warfare affect the classical security theory view of states actions?*

The research questions are based from my hypothesis that *classical security theory is not enough to understand or explain the new empirical phenomenon of cyber warfare on its own.*

## 1.2 Purpose of the paper

The purpose of this paper is to shed some light on cyber warfare as a new threat to national and international security. By using the realism security theory the natural focus of the paper are states and how their interaction with each other could be affected by this new threat. As evidence suggest, cyber warfare has already been used by states in actions against each other but is cyber warfare really a threat to national and international security?<sup>3</sup>

---

<sup>3</sup> Masters, Jonathan, *Confronting the cyber threat* , Council on foreign relations, 2011, retrieved 26 April 2011, <<http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577>>

By using the dominant security theory in international relations I hope to gain some explanations as to the relation of a new strategic interest of states as well as if it affects states interaction in the international system.

### 1.3 Method

For this paper I will use a hypothetical deductive method to compare a new empirical phenomenon to an already existing security theory. The problematic nature of cyber warfare could prove interesting points to the realism theory as well as the realism theory proving cyber warfare not to be an especially different aspect of international security theory.<sup>4</sup>

With my research questions being based on my hypothesis that cyber warfare cannot be fully understood through classical security theory I will test the hypothesis against the realism security theory which I have chosen to represent classical security theory. Being the dominant theory of international relations it seemed the most logic choice as it should provide one of the most comprehensive explanations.

As such, I will first present the basic elements of the realism theory and then explain the main divisions within it that I deemed necessary to include as they view state interaction to some extent quite differently. The focus of the paper is neorealism since classical realism focuses more on motivations in state interaction which I thought would prove perhaps more problematic to compare with cyber warfare. Though not explaining every argument and feature of the different divisions within the realism theory, I have tried to incorporate as many relevant and characterizing aspects as possible to provide a wide range of views to understand cyber warfare by.<sup>5</sup>

Following the presentation of the theoretical framework I will explain the basics of cyber warfare on how it can be understood and possible solutions to decrease the current weaknesses it presents to states. Again there are many aspects

---

<sup>4</sup> Teorell, Jan & Svensson, Torsten, *Att fråga och att svara*, Liber AB, Malmö, 2007, p. 48-9

<sup>5</sup> Glaser, Charles L., "Realism" in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 17-8

left out but since the requirements to explain the research question revolves around a state centered view, many arguments focusing on organizations and individuals could naturally be left out.

The analysis section will then present my findings on the relation between cyber warfare and realism security theory and the weaknesses and strengths provided by explaining and understanding cyber warfare from a realist perspective.

### 1.3.1 Material and previous research

The previous research on the subject of cyber warfare is fairly limited and specific information regarding it is quite difficult to come across. Rather ironic is the fact that the only other paper I found that was related to this subject of trying to understand cyber warfare from the realism theory was blocked by my anti-virus program as it apparently decided the host site of the document was spreading malicious code. As such, I am unaware of previous conclusions on the subject. Most of the articles and papers discussing cyber warfare are all based on a few central facts that make it difficult to actually state much specific information. The material used in this paper is therefore based on largely the same events and what scientist and experts have deemed as evidence, or as close to proven as possible, as well as policies proposed by previous government employees on their views on how to secure cyberspace.<sup>6</sup>

Much of the information available is from sources from the USA which has led this paper to have a certain focus on that state as it is one of the few that can provide some level of insight into the dealings with cyber warfare and the focus of states intentions with it.

---

<sup>6</sup> Masters, Jonathan, *Confronting the cyber threat* , Council on foreign relations, 2011, retrieved 26 April 2011, <<http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577>>

## 2 Theoretical framework

National security is probably one of the top interests for most of the states on the planet. How a state achieves that goal however is open to argument which is exactly what the different security theories do. In this paper I will focus on the realism theory of security and how they view different strategies for a state to achieve it.

Even within the dominant theory of international politics, or probably even because it is the dominant theory, there is a certain division on how to view and interpret different actions by states. I will present both classical realism and neorealism in this paper but I will be focusing mainly on neorealism and the division within neorealism. The division within neorealism is largely between the founder of neorealism, Kenneth Waltz, offensive realism and defensive realism which I will use to understand and interpret cyber warfare from different angles as they provide different ways of explaining and understanding cyber warfare.<sup>7</sup>

Arguably, the essential realism can be explained through the three different categories of *statism*, *survival* and *self-help*. Statism can be understood through the realism focus on states as the main actor in international politics and the concept of sovereignty meaning a state is the supreme authority within its territory. When security is achieved domestically, the state turns its attention internationally to maintain its security and achieve power within the anarchic international system. The realist view of the international system as anarchic can be explained with the absence of a supreme authority with control over the states of the world. In this situation states compete over both power and security in a zero-sum game meaning one states gain is another's loss.<sup>8</sup>

---

<sup>7</sup> Glaser, Charles L., "Realism" in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 16

<sup>8</sup> Dunne, Tim & Schmidt, Brian C., "Realism" in John Baylis, Steve Smith & Patricia Owens (ed.), *The globalization of world politics: An introduction to international relations*, 4<sup>th</sup> edn, Oxford University Press, New York, 2008, p. 100



One of the main critiques against the realist focus on states is on the concept of power and the ambiguous meaning of the word. To seek or possess power is mainly relational to that of the power of another state and to assess the power of a state is a complex task that is usually related to the military capabilities available. Furthermore, the concept of power can raise such questions as how to use acquired power and the ability to do so as well as the ability to influence and control the actions of others in the anarchic system by using ones power?<sup>9</sup>

The principle of survival is perhaps the foremost interest of the state according to realism and it can be seen as the precondition for all other goals of the state. As I will discuss later on, defensive and offensive realism have different views on the effects of the principle of survival has on the state, but in short, these include different arguments as to the level of risk a state is willing to take to ensure its survival. State leaders faced with the responsibility to protect their state often face a heavy burden and realism views them as having an “ethic of responsibility”. In short, this explains as leaders being aware that individual immoral acts could be necessary for the greater good of the state. Some of the critiques against this principle include the lack of guidelines for how to “weigh consequences” and that states leaders are considered to have an alternative ethic in international politics.<sup>10</sup>

The last category, self-help, is a combination of the previous two and presents a view on how states achieve survival. Since the international system is anarchic and the state cannot rely on any higher authority for their survival they must achieve it by providing security for themselves. This can be realized through a few different means but the most common ways are military buildup or the creation of alliances to counter another state or alliance power. I will be examining the view on alliances, balance of power and military buildup in depth later on so let’s conclude the principle of self-help by looking at the security dilemma which can be seen as the potential or probable effect of strengthening the security of a state. To understand the security dilemma it is probably necessary to explain the view realism has on states intentions. According to realists, states are

---

<sup>9</sup> Dunne, Tim & Schmidt, Brian C., ”Realism” in John Baylis, Steve Smith & Patricia Owens (ed.), *The globalization of world politics: An introduction to international relations*, 4<sup>th</sup> edn, Oxford University Press, New York, 2008, p. 101

<sup>10</sup> Ibid., p. 101-2

prone to distrust other states and their intentions. With that said the security dilemma can be understood as the spiral of insecurity created by states when intentions are interpreted differently, meaning one states military buildup to increase its security can be viewed as a decrease in the security of the neighboring states. An ironic effect of this strive for security is that neighboring states eventually end up being just as (in)secure as they felt before as the result of an arms race to counter the power of a stronger state.<sup>11</sup>

Having presented the basic elements of realism I will move on to explain the difference between classical realism and neorealism as well as the division within neorealism.

## 2.1 Classical realism

As previously stated the main focus on this paper will not be drawn from classical realism but I will in short explain the perspective of classical realism on international security theory.

The classical realism view on states behavior internationally can be seen as dependent on the nature of the individual state rather than on the international structure. Even more specifically the nature of man plays a part in the explanation of states actions. The interests of a state and the features of international politics can be traced to the nature of man which would then explain why states “feel” fear, strive for power and go to war as these conditions have their roots in human nature.<sup>12</sup>

As previously mentioned about the international system, classical realism does not dismiss the impact of the international structure on the state but with the classical realism focus on greedy states the international structure is to be viewed

---

<sup>11</sup> Dunne, Tim & Schmidt, Brian C., "Realism" in John Baylis, Steve Smith & Patricia Owens (ed.), *The globalization of world politics: An introduction to international relations*, 4<sup>th</sup> edn, Oxford University Press, New York, 2008, p. 102-3

<sup>12</sup> Ibid., p. 95

more as an influence on the greedy states ability to expand rather than being the cause of it.<sup>13</sup>

To understand classical realism and to put the actions of greedy states in somewhat of a context I will provide a few explanations on the probable actions of the greedy states. The greedy state is a state looking to expand, increase its wealth or pursue power in some other way, usually more so than other states. Contrary to security-seeking states, which I will discuss in depth further on the greedy state often choose competitive politics as it sees potential gains and cannot achieve its goals without engaging other states in competitive politics. Likewise if faced with an arms race, the greedy state will most likely see the advantages of winning that race against a competitor as such a win would enable it to achieve its “greedy” objectives. With that said, greedy states does not necessarily engage in competitive politics with other states as too high a cost to achieve its goals can effectively deter it from such competition.<sup>14</sup>

## 2.2 Neorealism

In short, neorealism view states behavior as dependent on the international environment they exist in and as such look to explanations given through the limitations and possibilities of each state. The three different theories within neorealism that I will focus on in this paper all view states interaction with each other and likelihood of international competition or cooperation quite differently which, as I will explain, also has an effect on how security is achieved.<sup>15</sup>

### 2.2.1 Waltz’s neorealism

Kenneth Waltz laid the foundations of neorealism in 1979 with his book *Theory of International Politics* where he started looking for answers in the international environment that states exist in rather than the states themselves for providing

---

<sup>13</sup> Glaser, Charles L., “Realism” in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 28

<sup>14</sup> *Ibid.*, p. 29

<sup>15</sup> *Ibid.*, p. 17-8

answers. One of Waltz's core assumptions is conjoined with one of realism as a whole, namely that all states prioritize their own survival. With this in mind, perhaps ironic is the fact that Waltz also argues that states have an inclination towards conducting competitive politics internationally. Even though the individual interest of the state might not be in opposition to another states interest, viewed collectively, this will generate arms races and the creation of alliances.<sup>16</sup>

With the international system being anarchic and states resorting to the condition of self-help, states facing dire consequences have a tendency to pursue policies that enhance their defensive capabilities and are equally reluctant to pursue policies that reduce those capabilities. In Waltz's view of realism, the future motives of a state are also uncertain and this only increases the difficulty of breaking out of the competitive system they are part of. One solution to this could be a mutual agreement between states that somehow ensures their continued security but the risk of a potential opponent cheating the agreement or even breaking it could make it a risky venture.<sup>17</sup>

So how do states achieve security and protect itself from attack? The simple answer is power, that can be manifested through economic resources, territory (and its population) and probably most evidently – military capabilities. To obtain more power or better defensive capabilities, a state has the options of external and internal balancing. Internal balancing has the state increasing its own military and economic capabilities while external balancing utilizes other states resources by forming an alliance with other states. The big drawback of forming alliances is that a state risk of being dragged into the war of an ally that could have been avoided had it not been for the alliance.<sup>18</sup>

There is an alternative to forming a balancing alliance. Where the balancing alliance has a state joining the weaker side of an alliance in order to counter the power of a stronger side, the *bandwagoning alliance* is about the opposite where a state joins the stronger side. According to Waltz's neorealism, a state is more likely to go for the balancing alliance rather than the bandwagoning alliance. The

---

<sup>16</sup> Glaser, Charles L., "Realism" in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 20

<sup>17</sup> Ibid., p. 20-1

<sup>18</sup> Ibid., p. 21

main argument for this is the contribution of power the state brings to the alliance. In a balancing alliance, a state is a necessary member to counter the other side's power while the bandwagoning alliance already is sufficiently strong and the state therefore don't contribute an essential part to the collective security of the alliance. In the worst case scenario of the bandwagoning alliance, the state can even be attacked by its own allies and as a result, probably have more to gain from joining the balancing alliance, even though it might not mean an advantage in power.<sup>19</sup>

### 2.2.2 Offensive realism

The offensive realism theory and its leading proponent John Mearsheimer provides a slightly different view on acquiring and using power compared to Waltz's theory. In addition to states being uncertain about the intentions of other states, offensive realism argues that states should also assume the worst in the intentions of other states. As a result, states are engaged in a constant clash in an attempt to acquire more power to increase their own security. This is termed *power maximization* and the logic behind it is quite simple. More powerful states stand a better chance of defending themselves and ensuring their own survival and with the same reasoning, the most powerful state of them all, the hegemonic state, is the most secure and should be the ultimate goal of a state to achieve if the probability of success is reasonable.<sup>20</sup>

Another argument provided by offensive realism as to the competitive nature of the international system is the tendency toward *buckpassing* within alliances. The concept of buckpassing comes from the difficulties pointed out in managing alliances. As states within an alliance can be geographically separated, disagree on the actions of the alliance or simply how to share the costs of potential fighting, states have the option of buckpassing within the alliance. So in short, buckpassing is the choice of a state to not take any course of action to balance out the power of another side. A few reasons for a state to choose buckpassing

---

<sup>19</sup> Glaser, Charles L., "Realism" in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 21-2

<sup>20</sup> *Ibid.*, p. 22

includes hoping for the neighbors of an expansionist state to balance out its power by themselves or viewing the balancing actions against a state not probable to succeed or to come at too high a cost. With this said, offensive realism acknowledges the fact that major powers do not always pursue competitive politics as the balance of power often forces powerful states to consider the reaction to their moves. If the risk of their potential gains is too high then they are more likely to wait for a more favorable moment.<sup>21</sup>

### 2.2.3 Defensive realism

Though sharing many of the assumptions of offensive realism and Waltz neorealism, defensive realism provides a different explanation on how a state can provide and achieve security for itself. The most obvious difference is that defensive realism recognize cooperation and restraint as options for achieving security and therefore view the international system to not have the same kind of competitive behavior as offensive realism and Waltz realism do.<sup>22</sup>

To understand how states in the international system can reduce the risk of insecurity and competition, the defensive realism looks to the security dilemma. If a state knows the intentions of another state or accurately identifies it as one of the greedy or security-seeking states, then much of the interstate problems would be removed. As the difficulty of assessing the intentions of another state increases, so too does the insecurity of its neighbors. One way of solving or at least assessing the intentions of a state is to look to its capability to attack and defend. A state with more defensive than offensive capability provides a larger degree of security to its neighbors than the opposite which then makes the state secure without risking making other states insecure.<sup>23</sup>

The intensity of the security dilemma can also have a great affect on the interactions between states, not just how they view each other's intentions. As defensive capabilities are stronger than offensive capabilities, so too is

---

<sup>21</sup> Glaser, Charles L., "Realism" in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 23

<sup>22</sup> Ibid., p. 24

<sup>23</sup> Ibid., p. 24-5

cooperation easier and agreements should pose less of a danger. When the opposite happens and the offensive capabilities outweigh the defensive capabilities, arms races would likely prove more intense, cooperation and agreements more difficult to achieve and competitive policies would be more likely.<sup>24</sup>

These interactions between one states increase in security that can lead to the other states decrease of security is identified to possibly proceed in three different directions that all can result in deteriorating political relations. The first is the military response of the weaker state to the newly acquired military capabilities of the stronger state. By building up its own military power, the weaker state matches or produces an advantage in military capabilities to that of the previous stronger state which ends up in at least on the states being less secure than before or possibly even making both sides less secure as the combined power of the acquired military capabilities of both states has a greater offensive capability, leaving them both more vulnerable to attack. The second explains how the insecurity of the rival state can lead to political conflict or even war. As the weaker state tries to match the stronger states power, drastic options are considered that might include grabbing territory from the stronger side. These options would be considered because the state is more likely to engage in risky policies to regain its security. Lastly, the buildup of the now stronger side can convince the weaker side that its intentions as a security-seeking state has changed and to cooperate with a greedy state can be too risky which opens up for more competitive policies.<sup>25</sup>

As shown above by the risks of competitive policies, defensive realism sees cooperation as an alternative means of gaining or keeping security. As opposed to risking competition with another state, cooperation has the advantage of gaining better political relations that in turn can help convince other states of its intentions. By looking at the example of offensive versus defensive capabilities of

---

<sup>24</sup> Glaser, Charles L., "Realism" in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 26-7

<sup>25</sup> *Ibid.*, p. 25

a state, an example of cooperation is arms control agreements that mainly limit the offensive capabilities of a state can bring greater security to all involved states.<sup>26</sup>

To convince other states of their security-seeking intentions, states willing to engage in cooperative policies might have to send a “costly signal” of their credible intentions. This “costly signal” would be in the form of an action that is less costly for a security-seeking state than a greedy state as the latter might have reasons to mislead other states to leave them vulnerable. Such a signal could (again) be an arms control agreement that limits the offensive capabilities of states, something the greedy state would be reluctant to agree upon as that would create problems for their expansionist interests.<sup>27</sup>

Even with the advantages of cooperation there are still potential dangers. As previously mentioned, states can cheat on agreements making the cheated state more insecure. To control an agreement and minimize the effects of potential cheating, monitoring the agreement can provide the states with enough time react even if the agreement is violated. If greedy states and security-seeking states cooperate, there is a risk that the greedy state questions the determination and capability of the security-seeking state. Naturally, certainty about the motives of the cooperating states is therefore an advantage.<sup>28</sup>

---

<sup>26</sup> Glaser, Charles L., “Realism” in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 25

<sup>27</sup> Ibid., p. 26

<sup>28</sup> Ibid., p. 26



## 3 Cyber warfare

We are living in a world that is becoming increasingly more interconnected and the internet has played a large part in that development. People can chat with their friends on opposite sides of the globe, upload videos for the world to see and trade on stock markets in other countries. Of course, some countries are more connected to, and dependent on, the internet than others. Developed countries have a much higher percentage of internet users in relation to their population than developing countries. With the simplicity of connecting to the internet and the large number of users in the world come great risks from those with malicious intent on the internet that become evident just by looking at the antivirus software installed on most computers.<sup>29</sup>

### 3.1 Understanding cyber warfare

To define the term “cyber war”, I have chosen to use the same explanation provided by Richard Clarke and Robert Knake. As they explain “...it refers to actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption”.<sup>30</sup>

While cyber war largely remains elusive to this day, experts on the area suggest it has already taken place and evidence already point out the weaknesses of states in cyberspace. Two events both argued to be the start of cyber warfare are the Russian invasion of Georgia in 2008 and the Stuxnet worm, first discovered in 2010.<sup>31</sup>

---

<sup>29</sup> Vatis, Michael, “The next battlefield”, *Harvard International Review*, vol. 28, no. 3, 2006, p. 56

<sup>30</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 6

<sup>31</sup> Masters, Jonathan, *Confronting the cyber threat*, Council on foreign relations, 2011, retrieved 26 April 2011, <<http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577>>

What makes the Georgian case significant is the fact that almost the entire country got shut out from the internet. Georgia's connection to the internet runs through Turkey and Russia and shortly before the Russian invasion began, the routers sending information to and from Georgia was so flooded by traffic that no outbound traffic from Georgia could pass through. The result was that Georgia was effectively cut off from the world (at least through the internet).<sup>32</sup>

The Stuxnet case is perhaps even more interesting as it produced physical damage. Though much of the information about Stuxnet is still unknown, analysts suggest heavy state involvement and point out both the USA and Israel as the possible creators. Iran seems to have been hit the worst by Stuxnet as reports indicate the Iranian nuclear program suffered damaged centrifuges as a result of the specific control systems targeted by Stuxnet.<sup>33</sup>

These are perhaps the two cases that have received the most attention in regard of cyber warfare. Without delving too deep into the technological part of the internet, what makes it vulnerable and why is cyber warfare possible? First of all, the world is connected in a way that has made production spread across many companies and states. Journalist and author Thomas Friedman spends six pages of a book tracing the production of his newly ordered laptop all the way from his phone order to its delivery at his door. In the short version, he finds that through the entire supply chain, around four hundred companies stretched across three continents had been involved. While also an argument for the cooperation of states, this also increases the possibilities of cyber warfare or at least works to the advantage of the countries involved in the production. The simple explanation to this is the possible introduction of vulnerabilities that could be exploited in a computer, router or similar product.<sup>34</sup>

Second, so called *trap doors* extend the argument above. A trap door is a vulnerability built into a computer program so that programmers can return and change the way the program works more easily. These trap doors can exist both

---

<sup>32</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 18-9

<sup>33</sup> Masters, Jonathan, *Confronting the cyber threat*, Council on foreign relations, 2011, retrieved 26 April 2011, <<http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577>>

<sup>34</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 86-8

intentionally as well as unintentionally and there is a possibility for unauthorized personnel such as hackers to find these trap doors and gain full access to programs. The larger the program, the larger the code that governs how it works which in turn adds to the risk of unauthorized access.<sup>35</sup>

Third, there is the placement of *logic bombs* within programs. Simply put, a logic bomb can be placed unnoticed on a computer by someone using a trap door and when the need for the logic bomb arises, it can erase an entire computer or send wrong signals through a computer to, for instance, force an electric grid to overload or even destroy itself. The concept of the logic bomb was created in the early 1980's by the CIA during the Cold War and implemented into a program before the KGB stole it and used the program in Soviet oil pipelines. Shortly after operations with the Soviet pipeline began, the program installed by the CIA forced an overload and the resulting explosion was the largest non-nuclear explosion recorded to date. That happened thirty years ago and as long as machinery or a computer is connected to the internet, anyone with knowledge can today place a logic bomb.<sup>36</sup>

As a last example to prove the possibility of doing damage through cyber warfare, I wish to illustrate an experiment conducted by the government in the USA. In the experiment, hackers attempted to, and gained, access to a one of the standard generators powering the electrical grid in the USA. With the hackers being only one keystroke away from completely changing the operating procedure of the generator, the experiment was called off. With the same course of action in this example, there is an equal possibility of a hacker to gain access to other systems and, for instance, force a train to derail by changing the tracks or cause other critical systems to go offline.<sup>37</sup>

So I would dare to say that even though we might not have seen any large scale cyber warfare, the threat of it is real. In fact many countries have already created

---

<sup>35</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 91

<sup>36</sup> *Ibid.*, p. 92-3

<sup>37</sup> *Ibid.*, p. 100-1

cyber warfare units as part of their military structure but few yet possess the ability to conduct such a sophisticated attack as the Stuxnet.<sup>38</sup>

Apart from the possible dangers posed by cyber warfare, how can it be regarded in terms of security and vulnerability from a states point of view? There are a few interesting aspects I would like to point out. First, dependency on the internet is an important aspect for states as it allows for a more vulnerable society. The logic is simple as more parts of the infrastructure are connected; it is easier to access those networks for unauthorized use. In the USA, the Department of Homeland Defense has identified eighteen sectors as critical parts of the infrastructure and all eighteen are relying on the internet for its functionality.<sup>39</sup>

There is no easy way to accurately assess the cyber warfare capabilities of a state as many factors play a part. In short, those factors can be summarized as offensive power, defensive capability and dependency on systems connected to the internet. As these factors all play a part in regard of the relative power of a state in cyber warfare, simply looking at one of them cannot determine the cyber warfare capabilities of a state. To illustrate this I have chosen to use a chart from Richard Clarke and Robert Knake.<sup>40</sup>

<b>Nation</b>	<b>Cyber Offense</b>	<b>Cyber Dependence</b>	<b>Cyber Defense</b>	<b>Total</b>
USA	8	2	1	11
Russia	7	5	4	16
China	5	4	6	15
Iran	4	5	3	12
North Korea	2	9	7	18

Looking at the different scores of the states is not the focus of the chart in this paper but instead to illustrate the relative capabilities and the total score which

---

<sup>38</sup> Masters, Jonathan, *Confronting the cyber threat*, Council on foreign relations, 2011, retrieved 26 April 2011, <<http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577>>

<sup>39</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 145

<sup>40</sup> Ibid., p. 147

present an idea of how total capabilities is dependent on the three different factors. Richard Clarke and Robert Knake have assessed the scores on their own but instead of explaining the meaning of the different scores; I will leave it as a hint to how capabilities can be viewed in terms of cyber warfare. As the total score hints, the most effective at offensive warfare is not necessarily the most capable in a cyber war since simultaneous defense might prove difficult, especially if the dependence on the internet is high.<sup>41</sup>

Such a comparison of states is not without complications however. As is already being discussed by analysts is the possibility of nations hiring other states or organizations with cyber warfare capabilities to conduct their operations in cyberspace. Even while tracing a possible attack such as this to a state, it is not necessarily the state where the attack originated in that ordered or asked for the attack.<sup>42</sup>

Another vulnerability of states is the asymmetry created by public versus private ownership of systems essential to the state in a cyber war. By looking at the USA again we gain fairly good understanding of the problem. Not only is the USA one of the most internet dependent states in the world, it also relies heavily on private companies to supply the technologies used in infrastructure and, perhaps even more crucial, military systems and contractors of the military. Technologies used, especially in the case of the USA, are often off-the-shelf products than virtually anyone can buy. Using such products in matters of state defense is probably not a great idea in the long run. Iraqi insurgents hacked the video feed from a Predator drone in 2009 by using a cheap computer to access its unencrypted signal which both proves the point of the dependency on the internet as well as the not so safe systems being used by the most powerful military in the world. Needless to say, if the video feed can be accessed by unauthorized sources, then more advanced manipulation of the systems cannot be disregarded.<sup>43</sup>

---

<sup>41</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 148-9

<sup>42</sup> Ibid., p. 155-6

<sup>43</sup> Ibid., p. 226-7

## 3.2 Confronting cyber warfare

So some of the vulnerabilities and problems for the state from cyber warfare have been presented but what can be done about them and how would they affect the state? First and perhaps foremost is the problems of a cyber war likely becoming global as states, willingly or not, become part of it. By looking at how the internet is created and how it works makes almost all traffic from one state to another travel through states not necessarily involved in whatever information being sent. Actions conducted through the internet are easily routed through a state that is not intentionally targeting the affected state which makes identification more difficult and also involves state that possibly wishes to remain neutral in a cyber war. This is however a very convenient way of conducting semi (un)lawful acts that probably have to be addressed. By comparison is a physical military action that enters a state unlawfully on the way to the target state.<sup>44</sup>

Globalization aspects of cyber warfare also involve the issue of collateral damage. Unless the weapons used in cyber warfare are extremely sophisticated and targeted at specific installations or products, there is a great risk of weapons affecting the civilian population of a targeted state and even other states as well. As is often seen in malicious code on the internet, there is an interest to see such code spread to as many computers as possible. If targeting a state and wishing said state to become crippled as fast as possible, the weapons used would likely not only affect military installations (as a possible target) but also infect civilian infrastructure with damaging code and with the rapid spread, likely move to states all over the globe.<sup>45</sup>

Herein lays one of the most dangerous possibilities of cyber warfare as well. If intentionally or not, an attack on the financial institutions of the world could cause a total collapse of the economic system. To enter the stock exchange of a state and change ownership or even erase all data regarding companies and records of transactions, there is a great possibility of not only direct collapse of the economic system but also the loss of faith in the security of such a system that in some

---

<sup>44</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 201

<sup>45</sup> *Ibid.*, p. 242-3

regard could be equally destructive. To this end there really is a need for legal framework in regard of civilian and financial infrastructure within cyber space.<sup>46</sup>

To counter some of the vulnerabilities made possible by the globalized nature of the internet the issue of sovereignty could again be brought to attention. Though no one is the direct owner of the internet there is a potential solution as tracing of the information sent through the internet is largely possible. As control of everything sent on the internet is not only very difficult and a potential violation of integrity, there is a possibility to monitor information flows and identifying botnets (large number of computers used together in a coordinated attack) targeting different states. To make it a national responsibility to stop the traffic coming from these botnets, with disregard of a state being an intermediary or the source, could at least be a huge step in right direction to counter some of the threats posed by cyber warfare. The same principle could be used to force governments to accept responsibility of cyber activities carried out from within their state and eliminate much of the deniability that cyber warfare has today.<sup>47</sup>

There is also a possibility of limiting the vulnerabilities of cyber warfare by implementing an agreement similar to that of nuclear weapons. Though I would not go so far as to compare the possible effects of both weapons there is a great danger posed by cyber warfare that could be diminished before the cyber warfare capabilities of states expand too far. Potential scopes of such a treaty could be “no first use”, ban on cyber weapons that target civilians as well as financial sectors.<sup>48</sup>

Another point worth mentioning is how cyberspace is already being prepared as a potential battlefield and how the lack of legal framework as well as the negligence of both civilian populations and many state leaders allows it to continue without further attention. The USA has already found both trap doors and logic bombs within their networks and have at least hinted toward themselves being engaged in similar activities in cyberspace. Compared to placing physical military equipment inside another state as preparation of a conflict that may arise,

---

<sup>46</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 202

<sup>47</sup> *Ibid.*, p. 248-9

<sup>48</sup> *Ibid.*, p. 269-70

it is strange how little attention these findings received when reported by the USA media in 2009.<sup>49</sup>

---

<sup>49</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 202



## 4 Analysis

As previously stated, cyber warfare enables a certain asymmetry in power that possibly could change the way realism views the power of a state and the way they interact. I will first look at how cyber warfare can be understood and some of the effects of it on realism in general and discuss a few problems and advantages with it and then discuss it a little more directly from the three theories within realism I have focused on in this paper.

One of the largest problems brought on by cyber warfare to realism in my opinion is the concept of power. Even if power is defined as military capabilities, technological sophistication or financial assets cyber warfare presents both new threats and aspects to each of them. In my opinion cyber warfare brings a level of asymmetry to power regardless of how it is defined. If viewed in terms of technological sophistication then, as hinted in the state comparison table, different aspects play a part in what is regarded as a better power. The correlation between offensive capabilities, defensive capabilities and dependence on cyberspace all play a part in regard of technological sophistications impact on how cyber warfare is to be viewed. As a state with great offensive power might be feared in cyberspace it might also be extremely vulnerable because of the relation capabilities play on each other. For instance, North Korea might not have a great advantage over the USA in terms of offensive capabilities but they also have less to lose from engaging in cyber warfare as they are much less dependent on cyberspace for their infrastructure. This could act as a potential divider of power since traditional military might can be toppled or at least thrown off balance due to technological differences.<sup>50</sup>

Likewise is financial power also at risk of becoming asymmetrical in terms of power as cyber warfare has the potential to destabilize stock markets by using cheap computers to hack or erase economic information. This is of course less

---

<sup>50</sup> Glaser, Charles L., "Realism" in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 18

likely the more involved a state is in the international economic system but by looking at North Korea and the USA again, there is probably more power to be gained by North Korea in disrupting the stock markets of the USA than reversed.

The realist assumption of states assessing each other in terms of power and capabilities is also potentially more problematic with cyber warfare. It is comparably easy to assess the strength of military units in real life as opposed to cyber weapons. Capabilities in terms of cyber warfare are much easier hidden and weapons to be used should be much easier to hide if detectable at all. This could act as a both a deterrence to states and make them overconfident in their own abilities. One of the reasons to why there is so much preparation and so little talk about cyber warfare could be because of this. As no state completely knows the others capabilities in cyberspace, they regard it as a strategic interest to not risk their own security. Perhaps the threat of cyber warfare is also completely exaggerated because of the fact that it is quite unknown?<sup>51</sup>

With states being aware of their own vulnerabilities in cyberspace could also prove to be upsetting the balance of power. States with currently strong military capabilities could refrain from engaging other states as they are unwilling to risk a confrontation in cyberspace. A lack of will to take action internationally could make other states bolder as the avoidance of a state is noticed.<sup>52</sup>

The statism focus of realism is also a bit questionable with cyber warfare as the accessibility of the internet could make actors other than states achieve the same amount of power depending on the definition of the word. Conducting attacks through cyberspace could be equally effective as a physical attack and has the advantage of remote accessibility. With enough resources at hand, an organization could gain enough power in cyberspace to challenge at least smaller states. It is to some extent comparable to private military corporations already at work for instance in Iraq.

When discussing measures to secure cyberspace against its vulnerabilities there is also a certain degree of confusion on what to secure. Since securing a states interests in cyberspace involves so many networks and computers it is

---

<sup>51</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 191

<sup>52</sup> *Ibid.*, p. 156

problematic to clarify what layers of society to secure. To secure the entire state within cyberspace would be very difficult and expensive but if only some layers of society is to be secured then which ones? Most populations would probably not want their networks scanned from incoming and outgoing traffic just as little as they would want their regular mail to be inspected by some government agency. But if only government and military networks got secured then the state is arguably not secure. Though military installations do not provide direct protection to everyone in the society, the ability to not protect most, if not all, parts of a states infrastructure then the civilian population that makes up the state is not secure.

By looking at the integrity problem previously mentioned under the section of confronting cyber warfare I would also argue to some extent against the threat level of cyber warfare from a realist perspective. Survival being one of the foremost interests of the state in realism, then a threat from cyber warfare would produce a response to secure that domain against its vulnerabilities. If the perceived threat of cyber warfare is large enough, the integrity problem of restricting, controlling or monitoring certain parts of states networks would not be any problem. Since the debate on cyber warfare and how to confront it is still relatively elusive, that could be seen as evidence of its perceived threat level within the state.<sup>53</sup>

Of course this is dependent on how cyber warfare is viewed. Cyber warfare need not be that effective by itself if not used in conjunction with other elements such as military forces but as a tool of terrorism or extortion it could be effective. Since that is not the focus of this paper, however enticing to discuss further, the fact that organizations and similar small scale actors could amass the same amount of power as at least smaller states should prove a point to the statism focus of realism. I would argue that possession of small scale military equipment versus small scale cyber warfare equipment does not provide an equal balance of power. Consider again the example of the power generator experiment in the USA. The hacker that gained access to the generator and power grid could have forced an overload on the entire system and compared to the physical

---

<sup>53</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 162

requirements of the same task in real life, I would argue that the cyber option is cheaper and simpler meaning it is a more effective way of gaining power.<sup>54</sup>

When looking at the reason for states to create alliances, cyber warfare could provide states with a new form of resource to contribute for an alliance. Probably more a reason related to balancing alliances rather than bandwagoning alliances since cyber warfare by itself does not provide the opportunity to seize territory. When looking to balance a states power, the concept of cyber warfare power has the potential to impact the decision of what states to balance against and what state to join the balancing side. Previous balancing may have been focusing more on military capabilities and their physical strength but to counter a cyber threat could make countries with a lot of skilled computer specialists and technological sophistication more interesting choices rather than the amount of military equipment.<sup>55</sup>

An argument following the realism theory closely is the suggested national responsibility against botnets and cyber attacks originating or passing through a state. Even though it might present many states with problems to deal with such a responsibility it is still a sound argument in my opinion. Not only would much of the deniability be eliminated, making intentions easier to make out, there would also be, as the suggestion hints, a national responsibility to control what activities are undertaken in cyberspace within a state.<sup>56</sup>

## 4.1 Cyber war and Waltz's neorealism

I find that some of Waltz's arguments on states behavior are quite applicable to cyber warfare while fewer could be seen as problematic. While looking at the concept of power as a means for achieving survival and the way of acquiring it either through internal or external balancing there are a few issues both in favor

---

<sup>54</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 100-1

<sup>55</sup> Glaser, Charles L., "Realism" in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 24-5

<sup>56</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 178

and not in favor of Waltz's neorealism. By revisiting the former thought of states being aware of their weaknesses in cyberspace there is a certain risk the state refraining from pursuing its interests as the consequences could outweigh the gains. This could in my opinion be seen both as an argument in favor and against Waltz's neorealism as interests previously within reach of a state could be overlooked but at the same time it goes hand in hand with the concept of survival as the state knows its weakness and is unwilling to risk exposing itself to danger. In this point of view, cyber warfare could prove problematic as it adds a new form of power for states that could have an effect on the state interests.<sup>57</sup>

Cyber warfare's effect on the creation of alliances is only really empirically relatable to the NATO creation of a cyber defense center in Estonia as a result of a serious cyber attack on the state but I have not found any other suggestions to similar creation of specific cyber defense centers within alliances anywhere else. It could be viewed as two arguments in favor of both the balancing alliances focus of Waltz's neorealism as well as the concept of self-help. With Estonia suffering a serious attack through cyberspace the need for a cyber defense center within NATO alliance became apparent as it obviously lacked capability to protect its members from such an attack but also, with the lack of similar cyber defense centers states many states apparently look to themselves for their own security.<sup>58</sup>

Depending on the development of cyber warfare there is also a potential risk for states currently not excessively dependent on internet for their infrastructure. It is perhaps a little exaggerated scenario but developing countries looking to improve their infrastructure might reconsider developing in the direction of internet dependency as they could run the risk of having new vulnerabilities to secure, especially if opposing states already have an advantage in cyber warfare capabilities. Far-fetched as it might be, this could have an impact on the concept of self-help too as such developing states could risk not improving technologies and infrastructure that could boost their economic power. The same argument

---

<sup>57</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 158

<sup>58</sup> *Ibid.*, p. 17

could also be used to explain states incentive to seek alliances instead to counter their disadvantage within cyberspace.<sup>59</sup>

## 4.2 Cyber war and offensive realism

The potential impact of cyber warfare on the power maximization focus of offensive realism could provide new challenges to the theory. Similar to the emergence of nuclear weapons, cyber warfare could provide states with weapons that provide asymmetry to the concept of power. While not comparing the destructive power of the two weapons, cyber warfare capabilities are much more easily obtainable and could provide greedy states with the capacity to challenge those of previously superior military or financial capabilities. The present difficulties of securing the state against cyber warfare and the lack of legal framework makes a shift in the balance of power easier as states with a strong financial base or military capabilities become more vulnerable against “rogue states” that see advantages to be gained by resorting to destabilizing acts against states with weaknesses in cyberspace.<sup>60</sup>

The idea of states assuming the worst in each other intentions is also fully applicable to cyber warfare in my opinion. Most states in the world have, as previously mentioned, already started looking to cyberspace as a security interest. This could be because they do not wish to fall behind in the development of cyber warfare and risk a weakness to other states or simply because the intentions of other states are unclear and they suspect adversaries would use cyber warfare against them. For major states, mainly the USA, this could provide a whole lot of states wishing to challenge it as states from the offensive realism point of view try to become hegemonic powers if the opportunity to so arise and the probability of success are reasonable. If states see an advantage against, for instance the USA, in

---

<sup>59</sup> Glaser, Charles L., “Realism” in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 20

<sup>60</sup> *Ibid.*, p. 23

cyber warfare, then they would use it to gain more power and make themselves more secure which, in this case, present the USA with a whole new threat.<sup>61</sup>

A great risk for states seeking additional power through cyber warfare against the states with major military capabilities today is the risk of retaliation with physical force. In seeing possibilities with disrupting for instance the USA in terms of attacks against the economy or power grid to cripple the state, there are still parts of military power that by themselves are more or less immune to the effects of cyber warfare. Future soldiers might be connected to the internet but soldiers today are not which makes cyber warfare perhaps effective at disrupting military responses but a committed response with physical force toward a state attacking through cyberspace would not be halted entirely by cyber warfare.<sup>62</sup>

As explained by the consideration of the balance of power in offensive realism the same above could also be a reason to why cyber warfare is not yet fully implemented into war. When the risks outweigh the benefits of an offensive action then states wait for a more favorable action and this provides an explanation in part to the preparation of the future battlefield with placement of trap doors and logic bombs in adversaries networks but also to the limited use of cyber warfare as the advantages of offensive actions in cyberspace not yet outweigh the risks.<sup>63</sup>

The balance of power is also at risk when looking at intellectual property and technological research advantages. Research takes time and money and with the relative ease such advances can be stolen through cyberspace, states risk losing their competitive edge in technologies and research by losing years of time and money in a matter of seconds. Compared to the investments, both in time and money, required to gain results in research to acquire the same knowledge, albeit illegally, by utilizing the internet there is a great risk for states in the forefront of

---

<sup>61</sup> Glaser, Charles L., "Realism" in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 22-3

<sup>62</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 157

<sup>63</sup> Glaser, Charles L., "Realism" in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 23

research to lose much of their advantages and thereby shifting the balance of power.<sup>64</sup>

### 4.3 Cyber war and defensive realism

When looking at the impact of cyber warfare on defensive realism one of my first thoughts was the security seeking states and the relation between offensive and defensive capability. As explained earlier the security dilemma could prove less severe if defensive capabilities of a state were more emphasized than offensive capabilities but this is, in its current form, problematic with cyber warfare as much of the defensive capabilities of cyber warfare is centered around the same ability as the offensive one. With the capabilities being intertwined in cyber warfare they naturally add to the problem of assessing another states intentions and a build-up to secure a states cyber dependency could result in other states regarding it as a greedy state with motives other than the direct security of its own assets within cyberspace.<sup>65</sup>

The balance of offensive and defensive capabilities also focuses a lot on physical factors that are difficult to apply to cyber warfare since, for instance, cyber warfare is tied to the internet which is not tied to any specific geographical spot. Distance and layout of terrain is therefore not an important issue with cyber warfare as anything connected to the internet is potentially reachable. This only serves to further prove the point of the offensive/defensive balance being intertwined in cyber warfare and makes capabilities in cyberspace more difficult to distinguish, arguably causing the severity of the security dilemma to be more difficult to assess.<sup>66</sup>

On a similar note is the build-up that is discussed throughout most of the book by Richard Clarke and Robert Knake. As they show, the build-up of forces in

---

<sup>64</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010, p. 237

<sup>65</sup> Glaser, Charles L., "Realism" in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 25

<sup>66</sup> *Ibid.*, p. 27



cyberspace, the book largely focusing on the USA and China, is a perfect example of how competitive policies also nurture potential vulnerability. By reallocating resources to also defend interests in cyberspace, not only do the states run a risk of disregarding other, perhaps more valuable interests, but they also risk ending up more vulnerable in cyberspace as the focus on cyber warfare provides new technologies and ways to deal damage to other states.<sup>67</sup>

If following the defensive realism idea of cooperation rather than competition there are also a few points that could generate additional problems to that argument. States willing to engage in arms control agreements should according to defensive realism adopt some form of monitoring to the agreement to decrease the risk of an agreement being cheated on. One problem with such monitoring on cyber warfare is the distinguishability of what is to be regarded as a weapon. Potentially any computer connected to the internet could be used with malicious intent.<sup>68</sup>

Similarly, if states is to balance against threats and not power, as argued by defensive realists, cyber warfare result in problems for that argument as well. Unlike assessing the physical military forces of an adversary state it is much easier to hide cyber weapons from another state. Satellites and spy planes have the ability to photograph number of tanks and their destructive power is easily measured. Weapons in cyber warfare could not only be easily stored on a USB-drive there could also exist trap doors and logic bombs within opposing states networks that are virtually undetectable. With threats being more easily hidden some of the argument of not increasing the security of a state to risk insecurity of another state is lost as a build-up of cyber warfare capability could be more easily hidden and therefore not producing an equally perceivable threat for a state to respond to.<sup>69</sup>

With the nature of cyber warfare being largely uncertain as of yet could however work to the advantage of defensive realism. Difficulties in distinguishing offensive or defensive capabilities, risks of changes in the balance of power and

---

<sup>67</sup> Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010

<sup>68</sup> Glaser, Charles L., "Realism" in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010, p. 26

<sup>69</sup> *Ibid.*, p. 18

states not looking to be viewed as greedy states are all factors that could push states toward cooperative policies. Of course this argument mainly applies to security seeking states since greedy states would view the potential of cyber warfare as tool to be used.

## 5 Conclusion

Cyber warfare seems to present some new challenges to the realism theory as it could apply changes to how some of the core features of realism are understood. How the concept of power is measured is one the features that probably will be influenced by cyber warfare entering states security interests. As cyber warfare adds a level of asymmetry to the concept of power by enabling states to acquire and challenge previously superior states with a cheap and accessible technology, major states are definitively up for some challenge as how to secure their own dependence on cyberspace and keep their superior capabilities.

In terms of intentions, cyber warfare could also require new forms of cooperation for security seeking states as the current capabilities in cyber warfare are largely indistinguishable from offensively or defensively oriented. The difficulty of assessing capabilities at all also plays a part as most states already consider cyberspace a part of their strategic interest which testifies of few states willing to neither give up power nor risk their security within cyberspace.

Depending on how cyber warfare is viewed, as a form of power on its own or part of the military capabilities of a state, the potential impact of it on the international system is changed. In connection with physical military capabilities cyber warfare adds much potential but on its own it is probably more destabilizing to power.

Neither branch of the neorealism family can understand or comprehensively explain cyber warfare in my opinion but they are not being proven incapable of explaining it either. Cyber warfare will add problems to understanding the intentions of other states, the balance of power and severity of the security dilemma but these are all minor flaws that are easily corrected and likely explained by the fact that cyber warfare is a new phenomenon.

For what it's worth, I would argue my hypothesis partly proven right as the realism theory seems to experience trouble explaining and understanding cyber warfare completely as it adds new asymmetries to many of its features.

With many new books and articles are scheduled for release however and new information will likely provide deeper insight into cyber warfare and progress within the area of cyberspace, both regarding legal framework and how states confront it should prove a better explanation to this new phenomenon.

## 6 References

Clarke, Richard A. & Knake, Robert K., *Cyber war: The next threat to national security and what to do about it*, HarperCollins Publishers, New York, 2010

Dunne, Tim & Schmidt, Brian C., "Realism" in John Baylis, Steve Smith & Patricia Owens (ed.), *The globalization of world politics: An introduction to international relations*, 4<sup>th</sup> edn, Oxford University Press, New York, 2008

Glaser, Charles L., "Realism" in Alan Collins (ed.), *Contemporary security studies*, 2<sup>nd</sup> edn, Oxford University Press, New York, 2010

Masters, Jonathan, *Confronting the cyber threat*, Council on foreign relations, 2011, retrieved 26 April 2011, <http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577>

Teorell, Jan & Svensson, Torsten, *Att fråga och att svara*, Liber AB, Malmö, 2007

Vatis, Michael, "The next battlefield", *Harvard International Review*, vol. 28, no. 3, 2006