The digital destruction

A case study of Stuxnet within the theory of new and old wars

Hana Hamdouni
Swedish Defense University
Master's Program in War Studies
Spring term 2017

Supervisor: Fredrik Doeser

Abstract

The aim of this study is to examine the extent to which Stuxnet can be characterized as a new war, if at all. The cyber-attack is studied within the theoretical framework of Mary Kaldor's 'New and Old Wars', where the case has been analysed through the perspective of both conventional and modern wars. Stuxnet is the first cyber-attack that has managed to act in complete secrete during a long period of time and causing its target physical destruction, while hiding all the evidence that could lead to the malware. The significance with Stuxnet is not merely based on its sophisticated operation but rather to the selection of its target, which is the Iranian nuclear enrichment program. The cyber-attack has raised questions of vulnerability and lack of securitization that the world faces in these situations. Nonetheless, it is rather difficult to prepare and secure ourselves from such attacks, if we do not understand their nature.

After examining the aim, the actors involved and the method of Stuxnet, it becomes clear that that the cyber-attack contain features from both old and new wars.

Keywords: Stuxnet, cyber-attack, nuclear program, new wars, old wars

Contents

1. Introduction

Mankind have since the beginning of time fought with each other for various reasons, calculated strategies to maximize their benefits and used numerous of tools to defeat their enemy. Destruction, espionage and sabotage are common concepts in warfare and are as essential parts of war today as they were over thousands of years ago. Nevertheless, there are significant differences on the adaption of these approaches that have evolved over time.[1]

Causing destruction in a state and accessing valuable information through espionage, has usually required crossing the enemy's borders. Protecting territorial borders is therefore one of the most fundamental elements of securing a state's existence as the borders work as a barrier between themselves and potential threats.[2] However, if the enemy can cause states severe destruction without crossing their territory, the protection of borders, along with the understanding of the threats we might face, must be reviewed.

Cyber-attacks have caused several damages on numerous countries in the recent decade and none of these states were necessarily prepared for these attacks. In 2007 Estonia was the victim of a wage of cyber-attacks, lasting for three weeks and targeting the Estonian government, Internet infrastructure, banking and media[3]. Georgia faced similar cyber-attacks against their media and some of their main communications channels in 2008[4]. In 2009 China was accused of releasing a cyber-spying program targeting over 100 countries and accessing valuable information.[5]

However, in 2010 a revolutionary cyber-attack took place and was later referred to as the world's first digital weapon.[6] Iran discovered in 2010 that their nuclear program had been attacked for at least a year without their knowledge by a cyber worm, later known as Stuxnet. The cyber worm

[1] Hamdouni, Hana (2017), "Iran's military cyber capability after Stuxnet", p.3

[2] Williams, John (2016). "The Ethics of Territorial Borders: Drawing Lines in the Shifting Sand", Palgrave Macmillan, p.1

[3] Geers, Kenneth (2011), "Strategic Cyber Security", ISBN, p.84

[4] Shackelford, Scott J (2014), "Managing Cyber Attacks in international Law, Business and Relations: In search for Cyber Space", Kelly School of Business, Indiana University, p.171

[5] Sood, Aditya and Enbody, Richard (2014)," Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware", p.5

[6] Zetter, Kim (2014) "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Buisness"

aimed at destroying the uranium enrichment in Iran to limit the capabilities of their nuclear program, and thus prevent a potential nuclear weapon.[7] Even though several countries have been victims to diverse cyber-attacks prior to the attacks against Iran in 2010, Stuxnet is argued to be the beginning of a new war era.[8]

1.2 Research problem

Mary Kaldor argues that war has adapted a new character in the post-Cold war era. She addresses several features that characterizes new wars, where one of the main targets is to achieve political goals instead of attaining geographical territories, which is usually the aim of conventional wars.[9] Not to forget one of the key arguments of Kaldor's, which is that these wars need to be understood within the context of globalization.

Numerous studies have been conducted on cyber-attacks and their relatively new role in conflicts. There are several articles and researches about Stuxnet that discusses various aspects and issues regarding the cyber worm. Some researchers, like Ronald C. Dodge, Lynn Futcher (2013)[10] and James Barret (2015)[11] discussed Stuxnet as a digital phenomenon that derives from the increasing dependence on technological means. Others, such as George Loukas (2015) [12] and Dorothy E. Denning (2012)[13], have instead focused on the impact of the cyber worm[14].

However, there are no studies concerning the character of Stuxnet from the new and old war perspective. In the era of globalization and advanced technological developments, it is important to understand that the threats we are facing today are different from what they used to be.

If we do not understand the nature of contemporary threats we will not be able to neither prepare nor protect ourselves from them.

[7] ibid, p.3

[8] Stuxnet: Computer Worm Opens New Era of Warfare", 60 Minutes http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/ (viewed Apr 1st, 2017)

[9] Kaldor, 2013, pp.73–74

[10] Dodge C. Ronald, Futcher, Lynn(Ed.) (2013) ""Information Assurance and Security Education and Training"

[11] Barret, James. Our Final Invention: Artificial Intelligence and the End of the Human Era, 2015

[12] Loukas, George (2015), "Cyber-Physical Attacks: A Growing Invisible Threat"

[13] Denning E. Dorothy, "Stuxnet: What has changed?", *Future Internet* 2012, *4*(3), 672-687; doi:10.3390/fi4030672

[14] Journal of International Affairs, Dorothy E. Denning, 2012, "Stuxnet: What Has Changed?", http://www.mdpi.com/1999-5903/4/3/672/htm (viewed Apr 1st, 2017)

As mentioned in the previous section, several countries have been victims of cyber-attacks prior to Iran in 2010. Nevertheless, none of these attacks have drawn as much attention as Stuxnet did. The uniqueness of the cyber worm is not merely related to the way it was implemented but also to the physical destruction it caused the target. Stuxnet had been destroying over a 1000 centrifuges and attained valuable information from the Iranian nuclear program for at least a year, while Iran had not the slightest suspicion of being attacked.[15] Stuxnet is therefore an interesting case to study in relation to Kaldor's theory of new and old wars. The research question that in this study is the following: *To what extent can Stuxnet be categorized as a New War, if at all?*

1.3 Disposition

The following section is discussing the theoretical framework for this paper and is divided into two main parts; old wars and new wars. The section that engages new wars has four subcategories and consists of a short introduction of the concept, followed by three characteristics of new wars; globalization, identity politics and method of warfare.

The next section is discussing the methodological framework for this paper. This section is describing the way the study is conducted, the choice of data collecting strategy and a short review of both strengths and weaknesses of the applied method.

The fourth chapter is a presentation of the applied theoretical framework and includes a sample of previous research that is relevant for this study. The empirical analysis is divided into three sections based on Mary Kaldor's characterization of old and new wars. Kaldor divides the concept of new wars in different categories, where each category consists of different attributes, while old wars are mainly based on Clausewitz perception of war. The empirical study contains of the following three categories: The aim, the actors involved and the method of warfare. Each part of the material will then be analyzed in the relevant category, for example; the material regarding the aim/s of Stuxnet will be presented in the first category. The final section is a conclusion of the study and will address an answer to the research question.

[15] Zetter, 2015, pp.2-3

2. Theory

As mentioned previously, it is of great importance to identify and understand the new threats the world might face along with the technological and political changes of our time. Mary Kaldor's theory of new and old wars is identifying and distinguishing traditional and modern wars. This is to provide a broader understanding of war in the modern era, which is a relevant theoretical framework for this study. New wars are a combination of wars (usually described as violence between political organizations and/or states for political purposes), the use of force between criminal organizations for private motives and the abuse of human-rights (states and/or political organizations using force against individuals).[16] [17]

However, there are opponents to the concept of 'new wars', such as Errol Henderson and David Singer, who argues that there are different types of warfare but that the essence of war is still the same. 'New wars' are discussed to be merely the result of combined warfare's, which has developed throughout the time due to technological developments amongst other circumstances. There are thus only one category of war and that is 'old wars'.[18] Kaldor agrees to this description to a certain extent and more specifically in relation to the use of different warfare's within new wars. Nonetheless, the combination of a variety of warfare methods is far from the mere feature of the concept. Kaldor argues that the concept of 'new war' mirrors the new reality that has emerged due to globalization and must therefore be understood within its context.[19]

[16] Kaldor (2013), p.2

[17] This should not be confused with the concept of 'Hybrid war' (introduced by Frank Hoffman, Conflict in the 21st Centurary: The Rise of Hybrid Wars, 2011), which is more concerned with the different types of war and the combination of warfare's. The concept suggests that wars today mainly has the same objectives as conventional wars, but what distingushies 'hybrid wars' is the variety of actors involved and the mixture of war methods. An example of a hybrid war is the conflict between Hezbollah and Israel in 2006, involving a state and a non-state actor, which acted in some degree on behalf of another state. The conflict contained a variety of warfare's including conventional and unconventional warfare's such as the use of guerrilla fighters.
Deep, Alex. Hybrid War: Old concept, New Techniques, Small War Journal, Mar 2nd, 2015
http://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques (viewed May 11th, 2017)

[18] Henderson, Errol., Singer, David. "New Wars" and Rumours of "New Wars", International Interactions: Empirical and Theoretical Research in International Relations 28:2, 2002, Abstract

[19] Kaldor, 2013, p.3

Kaldor argues that there are two timeframes that divides the concepts of new and old war, which are the post-Cold war era and the era prior to it. The wars in the post-Cold war era are conducted within the globalization process, they entail capabilities and aims that differ from conventional wars and requires therefore to be studied differently.[20] To understand and thus prepare for such conflicts, it is rather important to distinguish old wars from new ones and not the least to define what war is. According to Kaldor, the aims, involved actors and the methods of warfare are the main differentiations between old and new wars.[21] This will be explained further in 2.2 New wars, where the different aspects of the concept are presented.

In this study Kaldor's theory of new and old wars will be applied on the case of Stuxnet, to understand the cyber-attack that has been argued to be the world's first cyber weapon.[22] However, one cannot examine if Stuxnet can be defined as a new war, according to Kaldor's theory, without the understanding of what old wars are in the first place. The following section will therefore present Kaldor's definition of old wars, followed by her characterization of new wars.

2.1 Old wars

Kaldor's description of old wars is mainly established from Carl von Clausewitz perception of war. According to Clausewitz, war is a social activity that is managed and coordinated mainly by men who aim to impose physical violence towards the enemy. He argued that wars have their own unique logic and that all societies have their specific distinctive form of war.[23] The most common definition of war, used by military leaders and policy makers amongst others, is based on a certain phenomenon that evolved in Europe in the 1400th- 1900th century. This phenomenon is connected to the development of the modern state and has been through several changes throughout time. Some of the most significant phases it went through was the beginning of the

[20] ibid, p.1-2

[21] Kaldor (2013), p.7

[22] Joshua Alvarez, Center for International Security and Cooperation, *"Stuxnet: The world's first cyber weapon"*, Feb 3 rd., 2015 http://cisac.fsi.stanford.edu/news/stuxnet (viewed 18th Apr)

[23] Clausewitz, 1968, p. 202

rather small wars between the 1500th -1700thcentenary that was connected to the absolute state and the arousing of power it brought with it, to the revolutionary wars such as the American Civil War and the Napoleonic War in the 1800th century that were associated with the creation of nation-states, to the total wars in the beginning of the 1900th century and later to the "imaginary" Cold War in the late 1900th century that consisted of wars of alliances and blocks.[24]

All the above-mentioned changes are different types of warfare with variations of strategies, relations and military means. However, war was still acknowledged as the same phenomena and the different phases it went through were merely a diversity of shapes the event could adapt. The characterization of the phenomena of war is as cited by Kaldor: "...a construction of the centralized, `rationalized', hierarchically ordered, territorialized modern state."[25]

Nevertheless, the modern state as described above is leaving room for new shapes of sovereignty that have evolved from modern global developments and thus, making war an anachronism. [26] But what characterizes old wars? According to Clausewitz definition, war is a violent act that aims to enforce ones will over the enemy. Clausewitz defines actors in this context as states, and merely states, thus, the will that is imposed on the enemy using force, is representing the interests of the state. In other words, wars are fought due to state interests. [27] Although the aims in war might vary, due to the interests and the political motives that the states are seeking, the warfare is always the same. Clausewitz argues that combat is the only way of conducting a war and thus, absolute war is simply the solely method of defeating the enemy[28]

As previously mentioned, the perception of war that most people have today began along the formation of the modern state. Prior to that, citizen militias fought battles since there were no clear distinction between the state and the civilians. In the beginning of the European stage formation, armies were created and uniforms were made to distinguish the military from the civilians. This was mainly to distinguish criminal actors that used violence, from the state whom, were also using violence acts. The formation of the absolute state and their armies was the

[24] Kaldor, 2013, pp.15–16
[25] ibid, p.17
[26] ibid, pp.16–17
[27] Clausewitz, 1968, p. 101
[28] ibid, pp.646–647

foundation of the justification of war. What justified wars is therefore the interests of the states, if a state sought certain benefits that could be achieved through war, the act was legitimized.[29]

2.2 New wars

New wars contain features from the pre-modern era (such as the features of war described in 2.1) and modernity/post-modernity and is a phenomenon that mainly evolved in the post-Cold War era. According to Kaldor, the purpose for distinguishing old and new wars is to change the general conception of war. It is necessary to identify and recognize new wars since the world is facing a new reality. This reality, along with the new wars, needs to be understood within the context of globalization. Globalization is a comprehensive concept that portrays the diverse changes of the contemporary era, which consequently has affected the nature of war.[30] The process of globalization has contributed to a stronger interdependence between states in many regards. Two of the main sources to the interdependence in the international arena, is the spread of democracy and the financial cooperation's. This has led to fewer wars between nation-states, since war could risk more than it could benefit. [31] Herfried Münkler, in agreement with the above-mentioned argument, complements with emphasizing on the important role that both ethnicity and religion has in new wars. Münkler argues that the cultural, ethnic and religious movements are adapting the shape of social-ideologies and has been a way for mobilizing support for warring groups. This, amongst other events within the contemporary political realm, has decreased the presence of military interventions and is thus one of the main distinguishes of new wars.[32]

The following chapters are describing three of the main aspects within Kaldor's concept of new wars, namely: globalization, identity politics and method of warfare.

[29] Kaldor, 2013, p.19

[30] ibid, pp. 2–3

[31] Baylis, John., Smith, Steve., Owens, Patricia. The Globalization of World Politics. Oxford University Press 4th ed, 2008, pp.211-212

[32] Münkler, Herfried. The New Wars. 2004, pp. 1-2

2.2.1 Globalization

According to Kaldor, globalization is a paradoxical concept since it covers the complicated process that includes localization, fragmentation, homogenization and integration as well as globalization, at the same moment. [33] However, in a more specific definition of globalization, Kaldor describes it as an increased global interrelation in cultural, financial, political, military manners and finally, the developed nature of political authority. She argues that the globalization of the 1980's and 1990's was a new phenomenon, although globalization can be traced back to modernity or even prior to that. It has been debated that new wars are the outcome of the Cold War, which represents a void in power. The phenomenon can also be regarded as the result of the revolution in data processing, communication and information technologies and as the foundation for the interconnected world we know of today. [34]

According to Emile Simpson the inter-connectivity of globalization might destabilize the classic strategies of war. The fundamental aspects of Clausewitz definition of war can be challenged through the era of globalization. One of these challenges is the increasing distinction between military and political activities, which relays on the rising attention of the global audiences. The strategies in war are becoming more thoughtful of the global audience's judgement and is thus adjusting to suit such opinions. [35]

The new wars are evidently effected by globalization in a variety of aspects. Some of these changes includes the humanitarian and political involvement of non-governmental organization (NGO's) and international reporters, to mention but a few. However, what seems to be one of the main uncertainties in the debates of globalization, is the question of the future of "territorially based sovereignty"[36], in other words, the absolute state. States capability to be violent towards other states unilaterally has been vastly reduced and this is due to various reasons, among them being the interconnections between states such as military alliances and international arms trade

[33] Kaldor, 2013, p. 73
[34] ibid, p. 4
[35] Simpson, Emile. War from the Ground Up: Twenty-first Century Combat as Politics, 2012, p.68
[36] Kaldor, 2012, p. 5

and global norms that limits certain war acts in relation to international treaties. Thus, one could argue that the sovereignty of states is weakened, if not threatened by globalization.[37] But there are also other aspects that could threaten the absolute state in relation to globalization. If globalization has evolved the world through technological and ethical connections, the threats that the world faces must have changed as well in equivalence to its context.

2.2.2 Identity politics

In old wars, political motives (argued to be one of the main reasons for states involvement in wars) were essentially linked to ideologies[38]. Political motives are still argued to be one of the main reasons for the use of force, even in new wars. However, it is the definition of political motives that varies from the perhaps more traditional descriptions of the term. Kaldor presents two features of the new wave of identity politics in the context of globalization. The first one is global, local, national and transnational. There are for example Diaspora communities that increase their influences through the modern channels of communication and by the facilities of travel and can thus share and enforce their ideas. The second feature of identity politics is benefiting from the modern technology, where the media both delivers and constructs political and cultural norms. Horizontal cultures are evolving within the process of globalization, through new transnational networks that are established on transnational languages such as English, which is connected to well recognized companies like Mc Donald’s or Coca-Cola ™ and Arabic that nurtured modern TV channels such as Al Jazeera. [39] However, Kaldor makes a distinction between “Identity politics” and “Identity” in the context of conflicts in the globalization process. While the concept of “identity politics” is referring to religious, ethnical and racial movements, “identity” is a usage of labelling that are used as a source in political claims.[40]

[37] ibid, p. 6
[38] ibid, p. 8
[39] ibid, pp. 8–9
[40] ibid, p.79

2.2.3 The Method of Warfare

Another difference between new and old wars is the type of warfare used. In old wars the aim was more than often to occupy territories through military power and the use of force was therefore a crucial part of war. Although the use of force is still recognized in new wars, it is not a necessity to achieve the objectives. Battles are rather avoided, although used when necessary, in new wars and territories are sought to be controlled through political power instead. This might be implemented through i.e. the imposement of a certain political identity over a population while demolishing the other identities.[41] This can be correlated to the concept of smart power strategy, explained by Joseph Nye. He argues that in an increasingly decentralized political system, it is essential to combine soft and hard power strategies to achieve political aims. However, smart power strategies must be understood within its context for it to succeed. In other words, it is vital to study the tactics in relation to the aim.[42]

In the globalization era, the aims of war are not necessarily the same as in conventional wars and requires therefore requires a different method of warfare. Michael Sheehan argues that new wars are a product of the globalization process and consists of mainly two types of warfare. The first method of warfare in new wars can be found in countries like the U.S, where advanced technological means has been used towards traditional armies and resulted in dramatic conquests. This has led to debates regarding an eventual transformation of the conventional military affairs. The second type of warfare involves mainly non-state actors and the role of traditional military armies is therefore not as significant as they are in conventional wars.[43]

New wars can also be fought through the media, where a framework of a certain perception is created and widespread through i.e. televisions. In this regard, the media is a rather powerful instrument that can change and create the moral of the public opinion. Covering a specific aspect

[41] ibid, p. 9

[42] Nye, Joseph S. The Powers to Lead, 2008, p.84

[43] Baylis, John., Smith, Steve., Owens, Patricia. The Globalization of World Politics. Oxford University Press, 2008 p.211

of a conflict, where one part is portrayed as the victim, while the other part as the villain, sets the ground of what characterizes good and evil. Another aspect of new wars through the media is the frequent coverages of violent conflicts in wars, which weakens the moral and political restrictions of war since it appears as a regularity. [44] This brings us back to Nye's argument regarding the necessity of combining soft and hard power strategies in the globalization era, where both policies are significant depending on the context. Soft power as described above, can take shape in media coverage and shapes the moral discourse of the public and can thus contribute to a certain political control, whereas hard power might be relevant in inevitable battles.

Table 1.

As presented above, there are certain similarities yet crucial differences between new and old wars. The following table is a conclusion of the most distinctive and fundamental features of new and old wars:

Components	New War	Old war
The aim of war	• Political control • Private motives • Identity politics: ethnic, racial and religious objectives	• State interests, such as: territory expansion, political control and financial gains
The actor/s involved	• States (the target can vary, i.e. against individuals or other states) • Political organizations • Criminal organizations	• States against other states
The method of warfare	• Avoiding the use of force (although used if necessary)	• Use of force • Battles

[44] ibid, p.215

3. Method

This chapter is presenting the applied research design for this study, the strategy of data collection and the methodological framework for analyzing the data.

3.1 Research design

This study applies the case study design, where the case of Stuxnet will be analyzed as a single case within the theoretical framework. The characterization of case study design demands an intensive and in-depth analysis, while focusing on the complexity and the character of the studied case.[45] One of the distinguishing features of case studies, is that the researcher is generally concerned with identifying and illuminating the unique features of the studied case.[46] This research has a deductive approach, meaning that it is a theory-driven study where the propositions are deduced within the theoretical framework and a general knowledge of the case.[47]

Since the aim of this paper is to study the nature of Stuxnet in a detailed manner while examining to what extent it can be characterized as Kaldor's description of new wars, the case study design is a suitable method for conducting the study. Nonetheless, as much as this research design is appropriate for studying a case in detail, it is problematic to generalize the result.[48] This study is therefore aiming to be a contribution to this research field.

3.2 Qualitative content analysis

The approach of qualitative content analysis will be applied in the case study, meaning that the collected data will be studied in-depth to provide a profound understanding of the event. The purpose of qualitative data analysis is to interpret the meaning of the material in a

[45] Bryman, Alan. Social research methods, 4th edition, 2012, p.66

[46] ibid, pp.68-69

[47] Bryman, Bell, 2010, p.23

[48] Hamel, Jacques. Dufour, Stephane. Fortin, Dominic. Case Study Methods, 1993, p.27

methodological manner. Nevertheless, the strategy of qualitative content analysis is not able to provide an interpretation that covers all the material and the researcher is therefore required to focus on a specific aspect of the material that they desire to analyse.[49]

The research question is the compass that directs the qualitative content analysis towards a certain aspect of the collected material and it is this specific feature of the strategy that differs qualitative content analysis from other qualitative methods. Although qualitative content analysis cannot cover the meaning of all the material, it is an excellent method for analysing a specific matter in detail. Another beneficial attribute of this method is that it provides the possibility to analyse a large amount of data, since the researcher is usually concerned with a limited aspect of the information. [50] Qualitative research emphasizes on description and context[51] and is therefore a relevant approach for examining Stuxnet in the context of Kaldor's theory, which stresses that new wars requires to be studied within the context of globalization.

According to Margrit Schreier all methods of qualitative data analysis has their own method for overcoming the shortcomings of common understandings. The method of qualitative content analysis uses a two-stepped strategy. First, the researcher needs to explain the meaning of the material and divide the material into different sections of a coding frame. This will consequently lead to the second part of the strategy, which is the identification of the valuable parts of the material.[52] This methodological strategy is applied on this study, where the collected material is divided into different coding sections and analysed in relation to the aim of this paper. I will intentionally collect the relevant information in the collected material regarding Stuxnet, in relation to the theoretical framework, to answer the research question. As mentioned in the disposition, the empirical analysis is divided into three categories; the aim, the actors involved, and the method of warfare. The strategy of qualitative content analysis will assist in conducting an organized structure, since one of its characteristics, according to Schreier, is to focus on the relevant information of the material and classify it into different categories while using a coding frame. The three categories in the empirical section will therefore be used as the coding frame that will determine the relevance of the information in the collected material.

[49] Schreier, Margrit. Qualitative Content Analysis in Practice,2012, p.3

[50] Schreier, 2012, p.4

[51] Bryman, Bell, 2010, pp.392–293

[52] Schreier, 2012, p.5

3.3 Material

The data collection will be gathered from already existing material, which will consist of both primary and secondary sources. The primary sources consist of interviews and governmental protocols. One of the main primary sources in this paper is the documentary “Zero days”, directed by Alex Gibley. The documentary includes numerous interviews with a diversity of cyber-security experts, decision-makers and government officials. The secondary sources include previous research, governmental documents, public sources and articles.

The sampling of the data is based on the relevance of the content in relation to the aim of the research. This is a relatively common sampling strategy in case studies since the purpose is to investigate the case in a detailed manner.[53] However, since the data is collected through what I find is relevant to this research, which is a form of a subjective sampling strategy, the result cannot be generalized.[54] It is therefore of great significance to aim at collecting data from various reliable sources to minimalize the possibility of distortion. Nevertheless, the aim of this research is not to prove a certain assumption, but rather to examine if the new war theory can provide a suitable explanation of the cyber-attack in 2010. Due to this, I believe that the probability of being bias when collecting the data is rather low, although I am aware of the possibility.

3.4 Opalization

The reason for selecting to study the case of Stuxnet is mentioned in the previous chapters. Nonetheless, I have yet not explained why Stuxnet is examined as a war in the first place. To understand the nature of Stuxnet, it is rather essential to identify the different classifications of cyber-attacks as a term.

[53] Bryman, Alan., Bell, Emma. Business Research Methods, Published by Oxford University Press, 2010, p.12

[54] David, Matthew & Sutton, Carole. Social Research: An Introduction, 2011, p.197

According to Richard Clarke, former national US security director, there are four different phenomena's regarding cyber-attacks:

- Cybercrime: the theft of money.
- Cyber hacktivism: Includes groups like Anonymous and WikiLeaks that steals information from the original publisher for political reasons, or organized groups who are hacking for amusements.
- Cyber espionage: Arguably the most serious matter in the cyber realm and is the digital method of stealing valuable information.
- Cyber war: Although it is not that common yet, the US-led sabotage against the Iranian nuclear facilities, leading to physical destruction of the centrifuges through cyber-attacks, can be described as a war. [55]

In similarity with Clarke, Eugene Kaspersky argues that the physical destruction caused by the cyber worm and the political conflict between Iran and the US-Israeli alliance, can define Stuxnet as a cyber war.[56] I am conceptualizing Stuxnet in this study accordingly to the above-presented arguments.

The analyzation of the collected material is as previously mentioned divided into three categories based on the theoretical framework. These categories are adapted from Kaldor's conceptual definitions of new wars. Although Kaldor mentions a variety of features of new wars, I have chosen to focus on the purpose of war, the actors involved and the way of warfare. This selection is based on the belief that the above-mentioned categories are fundamental aspects that will assist in defining and characterizing Stuxnet in relation to the research question. As presented in table.1, new and old wars have different parameters in the description of wars. I will now present how these parameters and concepts are operationalized during this study.

[55] A. Clarke, Richard, The Economist's World in 2013 Festival, Dec 8th, 2012, https://www.youtube.com/watch?v=6_ek8mugOUc (viewed May 13th, 2017)
[56] Kaspersky, Eugene, "Cybercrimes with Ben Hammersley". BBC news https://www.youtube.com/watch?v=4oNnSStrc38 (viewed May 13th, 2017)

Identity politics is as mentioned in the theory chapter, one of the main goals in new wars. This concept is not difficult to measure since Kaldor has a rather concreate definition of the term, namely; a movement that claim power in relation to racial, ethnic and/or religious objectives.[57] *Private motives* and *political motives* on the other hand, are perhaps more diffuse. Both concepts are directly linked to the actors behind the war act, which makes it essential to define whom they are in the first place. The word 'private' in this context refers to the privately organized criminal groups and the private motives are thus the aims of such organizations. According to Kaldor the aims of criminal groups are usually concerning financial benefits[58]. In relation to cyberattacks, this definition is rather identical Clark's description of 'cybercrime' and I will thus measure the 'private motives' with the same parameters.

Kaldor refers to the 'political motives' as the aim of states and/or political organizations. This concept differs from the political motives in old wars, which refers to state interests and is usually concerned with territorial expansion, economical gains and political power through a state perspective[59]. In new wars however, the word 'politics' is understood within the context of globalization and is connected to the concept of identity politics. 'Politics' in this perspective is therefore related to culture, nation-tribes and/or religion[60] and will thus be used with these measures when conducting this study.

[57] Kaldor, 2013, p.7
[58] ibid., p.2
[59] Clausewitz, Carl Von. On War, 1968, pp. 119-120
[60] Kaldor, 2013, p.71

4. Stuxnet: New or old war?

Former U.S. Secretary of Defense, Leon E. Panetta argued that cyberspace have changed the way we live, providing people across the world to access information through various of communication channels, broadening the international economic sphere and contributed to a world full of possibilities. Along with these possibilities however, comes responsibilities and new risks. The internet is accessible for everyone, an open space which connects the world with a single click. Along with this openness, a new ground of war has evolved creating a new and limitless battlefield that makes it possible for enemies to harm states, citizens and their economy. [61]

In January 2009, officials from the International Atomic Energy Agency (IAEA) observed unusual circumstances at the uranium enrichment plant in Natanz, Iran. The centrifuges in Natanz were expected to remain working for about ten years, however due to the sensibility of the centrifuges Iran replaced up to ten percent each year. It was therefore relatively usual for Iran to replace around 800 centrifuges per year due to a variety of product defects and concerns regarding the maintenance.[62] Officials from the IAEA believes that approximately 2,000 centrifuges were replaced by Iran between 2009-2010, and although the cause of the damaged centrifuges was right in front of them it took them almost a year to detect it. [63]

Later in 2010, a Belarusian computer security firm detected a new type of malware, later known as Stuxnet. Although the discovery of a new type of malware was neither unexpected nor uncommon, the character and sophistication of Stuxnet was certainly different.[64]

In previous sections, the characterizations of new and old wars were presented within the theoretical framework. The following sections will be divided into the three main features of the wars, presented in table.1, where each category will be analysed in relation to Stuxnet.

By defining and analysing the aims, the method and the actors involved in Stuxnet, I will be able to investigate if the cyber worm can be characterized as a new or old war.

[61]Remarks by Secretary Panetta on Cybersecurity and Business Executives of National Security, New York, U.S. Oct 11th, 2012, Department of Defense, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136 (view May 13th, 2017)

[62] Zetter, Kim. 2014, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, p.1

[63] ibid, pp.2-3

[64] Rosenzweig, Paul. 2013, Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare, p.3

4.1 The aim of Stuxnet

The first reports claiming that Iran was developing nuclear weapons came in the 1970's and since then numerous of similar reports have accused the Iranian nuclear program for being a camouflage for a productive and advanced base for the creation of mass destruction weapons. Iran has since the time of the Shah, where the first accusations emerged, denied having the intentions of building nuclear weapons and argued that their nuclear activities are nothing but peaceful. Nonetheless, despite the large number of alarming reports against their nuclear activities, no conclusive evidence has been presented.[65]

However, after the fall of the Shah there has not been much data regarding Iran's nuclear facilities and the lack of transparency generated further accusations. Iran on the other hand, defended itself by claiming that they were act in accordance with arms control agreements and justified each new finding by referring to the development of a peaceful national nuclear power program. The outcome of these developments was a series of nuclear facilities and programs with unclear purposes. The suspicions against Iran's nuclear weapon program grew along with their nuclear achievements.[66]

Iran's nuclear program has been the victim of industrial sabotages for a long period of time. Due to its dependence on certain foreign modules, the nuclear program is in a particularly exposed situation. Despite the large amount of sabotages towards Iran's nuclear program, Stuxnet is by far the most advanced and destructive attack of them all. [67]

In June 2009, a vicious digital weapon was secretly unleashed on computers in Iran, finding its way into the vital systems in Natanz. [68] This digital weapon is now more known as Stuxnet. Stuxnet is a cyber worm constructed to target a certain service on a very exact sort of Siemens software that are used in the crucial systems of Iran's nuclear facilities. The software systems that were targeted are in control of the frequency converts, which regulates the speed of the centrifuges in the enrichment program. The cyber worm made these software systems command the equipment to speed in a destructive manner, leading to the centrifuges destroying themselves.

[65] Anthony H. Cordesman, 2005*," Iran's Developing Military Capabilities",* p. 94
[66] ibid p. 94-95
[67] (2011) Stuxnet: targeting Iran's nuclear programme, Strategic Comments, 17:2, p.2
[68] Zetter, 2014, p.3

Stuxnet is therefore argued to be specifically made with the intention to sabotage Iran enrichment program. [69]

According to the article “Stuxnet: targeting Iran’s nuclear programme”, the aim of Stuxnet is to mainly postpone Iran’s nuclear program through hindering their facilities to function, all this while acting in complete secret. The aim of Stuxnet is therefore not to sabotage Iran’s nuclear program in a manner that would eliminate its existence, but rather to delay it to buy the International community some time to pressure Iran through sanctions and negotiations and perhaps to plan for complementary policy measures. Instead of developing their already advanced nuclear facilities Iran would be occupied with reconstructing their damaged centrifuges and reviewing their cyber defense system. The vulnerable situation of Iran after Stuxnet, would therefore facilitate for the International community to impose their requirements. However, there has been other, more violent, methods for delaying the Iranian nuclear facilities than cyber-attacks. Several Iranian nuclear scientists have been assassinated through severe means such as bomb-explosions and mysterious traffic “accidents”. Cyber-attacks could therefore be argued to be a rather unconventional but un-lethal method for delaying the developments Iran’s nuclear program. [70]

In similarity with the article from IISS Strategic Comments, Kim Zetter argues that Stuxnet was specifically designed to target Iran’s nuclear facilities. Nevertheless, Zetter claims that the cyber worm was not merely constructed for delaying Iran’s nuclear program, rather it was unleashed for one purpose and that was to damage their uranium enrichment program in such a destructive manner that would hinder President Mahmoud Ahmadinejad from creating a potential nuclear weapon. [71]

Zetter is not alone with this explanation. Siemens cyber-security experts declared that Stuxnet was found in America, Australia, parts of Africa and all over Europe. Nonetheless, over 60% of the cyber-attack was targeting Iran alone. The geo-political situation of Iran was studied with the aim of finding correlations between the cyber-attack and the political circumstances. The

[69] (2011) Stuxnet: targeting Iran's nuclear programme, Strategic Comments, 17:2, pp.2-3

[70] ibid, p.3

[71] Zetter, 2014, pp.3-4

relatively brief research showed that Iran had recently suffered from unexplained gas pipeline explosions and mysterious assassinations of nuclear scientists. This in relation to the fact that the malware destroyed the Iranian nuclear centrifuges, made it rather evident that the aim of Stuxnet was to sabotage the development of Iran's nuclear program. [72]

Mariarosaria Taddeo and Ludovica Glorioso are in accordance with the above-mentioned opinions, arguing that the specific design of Stuxnet and the way it damaged the Iranian uranium enrichment specifically, are clear indications of the aim of the cyber worm- preventing Iran from building a potential nuclear weapon by sabotaging their nuclear program. According to Taddeo and Glorioso, this goal is something that the clear majority of the international community would regard as beneficial since it could prevent Iran from building a nuclear weapon and in that sense, Stuxnet has contributed to a safer world.[73]

Both security experts and diplomats have stated that Israel and Western governments believes that one of the most effective ways for slowing the Iranian nuclear program is through damaging it. By sabotaging crucial parts of the nuclear program, such as the uranium enrichment, Iran will be prevented from building nuclear weapons. The cyber security firm Symantec has conducted a study that confirms the sabotage theory based on the way Stuxnet is controlling the behavior of the equipment (the frequency converts). The aim of unleashing a cyber worm that specifically targets one of the world's most feared nuclear programs by systematically and secretively destroying the most crucial part of its developing system, cannot be other than eliminating the risk of Iran building nuclear weapons.[74]

Regardless of the criticism and tributes of Stuxnet's purpose, the majority, if not all, agree that the aim of the cyber worm was to sabotage the Iranian uranium enrichment program and thus prevent a potential nuclear weapon. This makes the aim of the cyber-attack highly political, which is a common denominator in both new and old war's in regard of the objectives of war.

[72] Symantec cyber-security experts: Chien, Eric. O'Murchu, Liam. Zero Days (2016), (DVD) United States, Magnolia Pictures

[73] Taddeo and Glorioso, 2017, *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Def4ence Centre of Excellence Initiative*, pp.215

[74] Maclean, William. *Stuxnet study suggests Iran enrichment aim: experts*. Reuters, Nov 16th, 2010 http://www.reuters.com/article/security-cyber-stuxnet-idUSLDE6AF0FX20101116 (viewed May 5th, 2017)

However, as presented in the theory section, political aims have different meanings in new and old wars. Limiting the capabilities of a state and preventing them from constructing and developing their military means, can be explained as political targets through a variety of aspects.

As the article from the IISS Strategic Comment and Taddeo and Glorioso argued, most of the international community would like to see a less developed Iranian nuclear program and are therefore more likely to approve of the aim of Stuxnet (dismissing its unconventional method). However, 'international community' as a term has been widely debated. The fundamental, yet somewhat unsatisfactory definition of the terms, is referring to a group of countries acting together as a unit.[75] This is in accordance with the United Nations definition of the term, where they explain it as a unity between states, intergovernmental organization and NGO's in the globalization era. The result of the international community can be seen in international law, global cooperation's such as economic, environmental and peacekeeping treaties. The international community is facing the same threats from nuclear weapons, climate change yet share the common benefits from the social and technological developments.[76]

However, not everyone agrees with this description. One of the debates regarding the term is made by Noam Chomsky who argues that the term is merely used by the US and their allies, while referring to themselves while aiming to increase their credibility and power.[77] Martin Jacques shares Chomsky's explanation and argues that 'international community' is a synonym to the West and is used by them to exalt and globalize their image. [78]

Regardless of which definition of the term one prefers, both explanations agree that it entails states. In this regard, the aim of Stuxnet can be argued to be linked to the interest of states, since the international community, according to the sources mentioned above, would like for Iran to have limited nuclear facilities. This would be in accordance to Clausewitz, who argued that states

[75] Cambridge Dictionary," International community" http://dictionary.cambridge.org/dictionary/english/international-community (viewed May 10th, 2017)

[76] Secretary- General Examines 'meaning of international community' in address to DRP/NGO Conference, 15th Sep, 1999, http://www.un.org/press/en/1999/19990915.sgsm7133.doc.html (viewed May 12th, 2017)

[77] Poellinger, Clemens., Stort publiktryck på Chomsky-föreläsning. Svenska Dagbladet, Sep 20th, 2002, https://www.svd.se/stort-publiktryck-pa-chomsky-forelasning (viewed May 10th, 2017)

[78] Jacques, Martin. What the hell is the international community?. The Guardian, Aug 24th, 2006 https://www.theguardian.com/commentisfree/2006/aug/24/whatthehellistheinternati (viewed May 12th, 2017)

interest is the main aim of war. Furthermore, Clausewitz argument regarding states interest is divided into different sections, among them being the power, financial gains and territorial expansions. Though territorial expansion is not relevant in the case of Stuxnet, since the target was the Iranian nuclear program, both political power and financial gains can be discussed.

The international communities interest in limiting Iran's nuclear facilities, is argued to be directly linked to defence policies since they want to eliminate the risk of new nuclear weapons. If that is the mere reason, one might ask why other nuclear programs and facilities such as Pakistan[79], North Korea[80] or Israel[81], have not been targeted in the same manner. It has been argued that the US and their allies' role in the Middle East is threatened by the dominating presence of Iran and if Iran develops nuclear weapons, the international community, assuming it is Chomsky's definition of the term, will not be as influential as they would like to be. [82]

In this aspect, the aim of Stuxnet can be interpreted as a way of achieving more power and can therefore be connected to both new and old wars. Nonetheless, it is the means of achieving power that distinguishes the wars from each other. In Clausewitz's explanation, power is usually connected with physical targets such as territorial expansions, which again, is not relevant in this case. New wars on the other hand, associates power to political control, which is aimed to be achieved without the use of force. It could be argued that the attacker imposed their will, which is to limit the Iranian nuclear facilities, and thus achieving a certain level of political control on the victim. In this regard, there might be more similarities with the characterizations of new wars since the political aim was achieved without the use of force. Nonetheless, the aspect of identity politics where movements of ethnic, religious and racial identities organizes to claim state power[83], is absent in the case of Stuxnet.

[79] Joseph V. Micallef, Jul 2nd, 2016, The Huffington Post "The other bomb: Pakistan's Dangerous Nuclear Strategy" http://www.huffingtonpost.com/joseph-v-micallef/the-other-bomb-pakistans_b_9180504.html (viewed 7th May 2017)

[80] North Korea's nuclear programme: How advanced is it?. BBC news, Jan 6th, 2017, http://www.bbc.com/news/world-asia-pacific-11813699 (viewed May 7th, 2017)

[81] Borger, Julian. The truth about Israel's secret nuclear arsenal. The Guardian, Jan 15th, 2014, https://www.theguardian.com/world/2014/jan/15/truth-israels-secret-nuclear-arsenal (viewed May 7th, 2017)

[82] The Middle East: Abstracts and index. Library Information and Research Service, 2006, p.225

[83] Kaldor, 2013, p.79

4.2 The actors involved

According to the computer security experts that have studied Stuxnet, it is most likely that a nation state/s is behind the attack and this is due to the amount of recourses, complexity and the risks of the cyber worm. [84] Vitaly Kamluk a director at Kaspersky Lab, agrees with this explanation and argues that criminals are usually interested in stealing money, while hacktivists usually have political agendas. Nation states on the other hand, are interested in valuable information or sabotage activities. Due to the target of Stuxnet, the cyber-attack is most likely the result of one or more nation states.[85] As mentioned in the previous section, several sources claim that Stuxnet is the result of an US-Israeli cooperation. However, despite these accusations against the US and Israel, none of them has admitted to the crime, which can only be expected in such a situation where the secret weaponized codes, like in the case of Stuxnet, can be deniable unlike the dropping of bombs.[86]

Nonetheless, there are some indications in the malware that supports these speculations.
One of these indications is the number "19790509" which was found in the code of Stuxnet. This number is argued to be the date of Persian Jewish businessman and head of Tehran's Jewish community's Habib Elghanian's execution in Iran. [87] Another, although rather weak, indication is the name "Myrtus" that appears in the code. It is believed that Myrtus is a reference to the Old Testament and more specifically to the Book of Esther, where Esther was described as the one who saved the Jews from the Persians. Nonetheless, the letter combination RTU found in MyRTUs, can also be defined as "Remote Terminal Unit", which is a common device that is frequently linked to Siemens controlling systems, also known as Supervisory Control and Data Acquisition (SCADA) systems. Nonetheless, the aim of Stuxnet and the political circumstances in the region makes Israel a natural suspect. Israel has both the motives, capability and

[84] Falkenrath, Richard on Bloomberg News
https://www.youtube.com/watch?v=VAXOTJkzGL8 (view May 13th, 2017)
[85] Zero Days (2016), (DVD) United States, Magnolia Pictures
[86] Hammersley, Ben. Cybercrimes with Ben Hammersley. BBC News
https://www.youtube.com/watch?v=4oNnSStrc38 (viewed May 13th, 2017)
[87] Bryen, D. Stephen. Technology Security and National Power: Winners and Losers, 2015, p.1-2

opportunity to conduct the cyber-attack towards the Iranian nuclear facilities, and so does the US.[88]

The New York Times reported that Stuxnet was developed by both the US and Israel who aimed at slowing the Iranian nuclear facilities. According to the article, members from the former US president Obama's national security team, confirms the suspicion of an US-Israeli cooperation behind Stuxnet.[89] Another indication of Israel's involvement in the launch of the cyber-attack, was on Israeli general Gabi Ashkenazi's last day at work where a video that included references to Stuxnet was presented. The video was a presentation of his achievements during his service, which fuelled the speculation towards Israel's involvement in the cyber-attacks even further. [90] In 2016, the US government accused Iran for being behind several cyber-attacks between 2011-2013, targeting a New York dam and U.S banks, which led to economic loses. The US claimed that the attacks were persistent and strategic and could therefore not be the work of individual Iranian hackers but rather the Iranian administration. Security experts have argued that these cyber-attacks are direct consequences of Stuxnet and that both the US and Israel might be victims of such attacks in the future due to their debated involvement in the cyber sabotage in Natanz 2010.[91]

This indicates that Stuxnet has created a counterattack, which resembles the perhaps more conventional features of war. According to Clausewitz wars craves counterattacks, where the defender is aiming to use counterattacks to primarily achieve victory but also to deter and protect the state from potential attacks.[92] However, it is not merely the counterattacks that resembles the perception of old wars but also the actors involved. Even though there are no official statements confirming the responsible actors behind Stuxnet, most sources agree that it is an US-Israeli

[88] Rosenzweig, Paul (2013), Cyber Warfare: How Conflicts in Cyberspace are challenging America and the World, 9-10

[89] Sanger, E. David. Obama ordered wave of cyberattacks against Iran. The New York Times, Jun 1, 2012 http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (viewed May 13th, 2017)

[90] Zorz, Zeljka. Israeli general claims Stuxnet attacks as one of his successes. Help Net Security, Feb 15th, 2011 https://www.helpnetsecurity.com/2011/02/15/israeli-general-claims-stuxnet-attacks-as-one-of-his-successes/ (view May 13th, 2017)

[91] Volz, Dustin., Finkle, Jim. U.S. indicts Iranians for hacking dozens of banks, New York dam. Reuters, Mar 25th, 2016 http://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WQ1JF (viewed May 13rd 2017)

[92] Clausewitz, 1984, p. 391

cooperation. It therefore seems reasonable to assume that all the primary actors involved in Stuxnet are states. In this regard, the involvement of actors in Stuxnet is in accordance with the perception of old wars, which argues that the main actors in wars are states.

New wars do recognize states involvements in wars as well, although within the context of globalization. According to Kaldor, government organizations are changing in the globalization process, where government activities within different departments are entailing privatized or semi-privatized arrangements. This has challenged the perhaps more conventional perception of a nation state. Governments in the contemporary globalization era are developing horizontal and transnational connections, which means that the decentralization of power that is usually seen in NGO'S can also be found in nation states. This means that the global political structure is evolving, where the link between nation states, NGO's and companies are more interconnected.[93]

This can be correlated to Iran's accusations towards the engineering firm Siemens (the industrial control system for the Iranian nuclear program) for assisting the US and Israel to launch Stuxnet. Carey Nachenberg, Vice president at Symantec Corp, referred to Stuxnet as a wake-up call for the world. Stuxnet bypassed all the acknowledged cyber security companies, which stresses the fact that it is extremely difficult to protect ourselves from such attacks. Seven different mechanisms were used in Stuxnet to spread its virus, these mechanisms are from Siemen's and are used for programing industrial systems, such as the PLC. Nonetheless, one of these software's had a default password that came from the manufacturer; Siemen's. Stuxnet broke through the defaulted password and could thus access the system. [94]

Iran's civil defence chief, Gholamreza Jalali requested a legally investigation of Siemens SCADA software's role in the case of Stuxnet. He argues that there are vital indications that the US and Israel could not have obtained the necessary information to target the SCADA software on their own and more specifically, without the assistance of Siemens. Siemens was accused for providing valuable information regarding the control system, such as maintaining a defaulted

[93] Kaldor, 2013, p.76

[94] Nachenberg, Carey. How a computer virus foiled Iran's nuclear program, CISAC Science Seminar, Apr 23rd, 2012. https://www.youtube.com/watch?v=DDH4m6M-ZIU (viewed May 18th, 2017)

password, of the Iranian nuclear program to the US and Israel, which facilitated the cyber-attack. [95]

Reviewing Stuxnet from this aspect, provides a possible recognition of the characterization of new wars that entails the involvement of both states and other global actors in war. The Iranian nuclear program and crucial information regarding its survival is dependent on an internet-based control system. Due to the nature of the internet, its openness and speed, the interconnection between a diversity of actors is not only inevitable, but also essential. The cooperation between nation states and a variety of other global actors, such as international companies and NGO's, is equally inevitable in the sphere of globalization. It could therefore be argued, despite the accuracy of the accusations regarding Siemens involvement in Stuxnet, that nation states and other global actors are interconnected in the cyber-attacks towards the Iranian nuclear facilities.

4.3 The Method of Stuxnet

A Zero-day vulnerability is a hole in the software that the owner or developer is not aware of. When hackers find this hole before the owner has the chance to even discover and repair it, it is referred to as a zero-day attack. The Zero-day attacks are used for espionage, instructing malwares and accessing valuable and classified information. The term itself is a referent to the anonymous character of the hole for everyone besides the hackers.[96]

Advanced cyber-attacks that are conducted by criminals and hackers has at the most one zero-day. Stuxnet on the other hand, had four zero-days in one single malware, which has never been seen before nor after Stuxnet. [97]In the case of Stuxnet, the zero-day vulnerability was used to spread a malware, which is a malicious software that is capable of undermining, stealing and sabotaging data. In this context data is defined as zeros and ones, meaning that malware is electrons undermining other electrons. The destruction of these electrons does not mean the mere

[95] Dehghan, Saeed Kamali. Iran accuses Siemens of helping launch Stuxnet cyber-attack. The Guardian, Apr 17th, 2011https://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack (viewed May 14th, 2017)

[96] "What is a Zero-Day Vulnerability?" PC tools by Symantec, http://www.pctools.com/security-news/zero-day-vulnerability/ (Viewed May 16th, 2017)

[97] Cybersecurity expert: Kaspersky, Eugene. Zero Days (2016), (DVD) United States, Magnolia Pictures

destruction of valuable data, but that actual physical objects that are managed by electricity might be equally sabotaged. [98]

Stuxnet attacked a Microsoft operating system, called SCADA. The computers that controls SCADA are usually not directly connected to the Internet, due to the valuable information it contains. This connection is usually avoided through an air gap between the SCADA controlled computer and the internet. Nonetheless, there are certain methods to avoid this air gap. There is a possibility to insert the malware on the sensitive side of the air gap, this however, can only be done by a spy. This is argued to be the case with Stuxnet, where the Siemens SCADA system is believed to have been infiltrated through a memory thumb drive. Stuxnet was deliberately avoiding attacking the non-centrifuges SCADA's since it could reveal its cover. This indicates that the developers of Stuxnet had significant information regarding the Natanz plant and the Siemens SCADA system, since the cyber worm could tactically avoid the gaps that could exploit its presence. [99]

Stuxnet is 20 times larger than an average code and contains almost no bugs, which is extremely rare. All the digital codes within Stuxnet were actively working towards a certain target to conduct the attack. It took the cyber-security experts months to even detect the secret codes, which is a process that usually takes a few minutes to implement with regular cyber-attacks. Viruses usually spreads through additional devices, such as damaged disks or files, Stuxnet was however different in that regard. One of the significant aspects of Stuxnet is that it spread and evolved the virus on its own, which means that the victim has no chance to protect themselves. The actors behind the attack could not go to companies such as Microsoft and ask them for digital codes, since that would expose them. Instead, the digital codes used in Stuxnet were stolen and could later be tracked back to two companies in Taiwan.[100]
Ralph Langner, one of the control security experts who analysed Stuxnet during the attack, argues that the malware was directly targeting Siemens computers and more specifically the Programmable Logic Controllers (PLC), which is a small computer that is connected to physical

[98] Hafemeister, David. (2016), Nuclear Proliferation and Terrorism in the Post-9/11 World, p. 314
[99] ibid, p. 14
[100] Symantec cyber-security experts: Chien, Eric. O'Murchu, Liam. Zero Days (2016), (DVD) United States, Magnolia Pictures

equipment's. This small computer runs a digital program, which controls the speed and actions of the equipment's. In the case of Stuxnet, it was used to control the speed of the motors of Iranian centrifuges in Natanz. Although the advanced malware had the ability to break through various of codes and thus control a variety of equipment's, it only targeted the codes that were directly linked to the motors of the Iranian nuclear centrifuges and ending up with destroying over a thousand centrifuges.[101] Stuxnet was therefore not designed to steal information or money, it was simply trained to infiltrate the Iranian industrial program and to literally explode their engines. [102]

It is rather evident to say that Stuxnet was not implemented using force and thus the method of warfare within the concept of old war, is not relevant in this specific case. New wars on the other hand, suggests that the method of warfare has changed since the Clausewitzian war era. Violence is avoided in new wars since the aim of these wars does not usually require force to be achieved. Instead of using force to attack the Iranian nuclear centrifuges, the damages were implemented through technical channels while avoiding anything that could draw attention to the malware. The cyber worm was specifically designed to hide its tracks while attacking, which indicates that the Clausewitizian understanding regarding the significance of battle in wars, was not just avoided but also unnecessary for the attacker to reach their aim.

Since globalization is a vital aspect of new wars, it is of great essence to understand the way Stuxnet was conducted within the context of globalization. The interconnected technological networks provide a unified platform of services, that most modern nation states depend on. Nonetheless, these very services might cause severe damages that can be conducted with a simple click. The computer software that Stuxnet was spread through is a common Microsoft device that is used by both individuals for private purposes and by nations states for critical and classified matters. Although the attackers could not use the original Microsoft codes to access the Iranian Siemen's computers, due to the risks, they were easily able to steal the appropriate digital

[101] Langer, Ralph. Att knäcka Stuxnet, 2000-talets cybervapen. TED Talk, Mar 2011 https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon?language=sv (viewed May 18th, 2017)

[102] Gibney, Alex. The Secret Cyberwar is Here: Director Alex Gibney on 'Zero Days' Documentary, Stuxnet & Cyberweapons (Video). Reasons, July 8, 2016 http://reason.com/reasontv/2016/07/08/the-secret-cyberwar-is-here-director-ale (viewed May 18th, 2017)

codes from other companies that are located on the other side of the world. This is simply because most actors, individuals, companies and nation states, use the same devices.

In this regard, it could be argued that the way Stuxnet was implemented is in accordance with new wars, both in relation to the method of warfare and within the context of globalization.

5. Discussion

The first section described the aim of Stuxnet, which according to the majority of the sources was to sabotage crucial parts of the Iranian nuclear program and thus hinder the construction of nuclear weapons. According to the article from IISS Strategic comments, the attackers were aware of the fact that the malware could not sabotage the Iranian nuclear program to the extent that it would deter them from developing the it. Stuxnet was rather a method that bought the international community some time to pressure Iran through i.e. sanction, to decrease their uranium enrichment and be more transparent in regard of their nuclear program. This would be more successful to conduct
while the Iranians were focused on their setbacks and could thus not afford further loses. Both arguments agree that Stuxnet targeted one of the most crucial part of the Iranian nuclear program and that the aim was to sabotage and hinder the development of their nuclear program and thus prevent the construction of potential nuclear weapons. In this regard, the aim is political since it is in the interests of nation states, sabotaging parts of another state's nuclear program to hinder them from developing what is feared to be nuclear weapons, can be argued to be a way of imposing the will of the attacker on the victim. This is in accordance with the concept of 'old war' since the main aim of war is to attain political objectives, although not in the sense of expanding territories but rather in aspect of increasing the state's political power.

Most cyber-security experts that has analysed Stuxnet, agrees that the cyber worm was not the result of common hacktivism or cyber-criminality but the consequence of a distinctive and authoritative state-cooperation. As mentioned above, the empirical analysis presented that Stuxnet is most likely conducted by two nation states, namely; the US and Israel. Neither of the states has admitted to the crime, which can only be expected in such situation. The signs within the malware, the geo-political situation between Iran and the allies US and Israel, along with statements from governmental officers, like in the case of Israeli general Gabi Ashkenazi, fuelled the suspicions towards and US-Israeli cooperation. The main actors in Stuxnet is therefore nation states, which is again in accordance with the concept of 'old war'. 'New wars' do recognize the involvement of states in wars, but argues that modern wars rarely involve just state actors. Iran has however, accused the software company SIEMENs for providing valuable information to the US and Israel, which made the cyber-attack possible. This can in a sense be argued to be in favour of new wars, since an international non-state actor might be included in this attack. Nonetheless, even if SIEMENs did contribute to the attack by providing information to the US and Israel, the main actors are still the nation states.

Although Stuxnet is neither the first nor the last cyber-attack, it is unique in many regards. Stuxnet is argued to have been implemented with a thumb drive by a spy, the cyber worm then evolved on its own and infected software's all over the world, where 60% of the virus were found in Iran alone. It operated under complete secrecy and hid all the traces that could expose its existence, which made the victim unaware of the attack. This led to severe damages of critical equipment's in the Iranian enrichment program and although Iran did eventually recover from the damages, approximately 2,000 centrifuges were sabotaged through the cyber-attack. Clausewitz argued that the aim of war cannot be reached without the use of violence and battles are thus a necessary component in war. Kaldor on the other hand, claim that the use of force is avoided in new wars and that the purposes of war can be achieved through other means. Stuxnet achieved its aim in relation to causing physical damages on crucial parts of the Iranian nuclear enrichment program, without the use of violence and is thus in accordance with Kaldor's description of method of warfare in new wars.

6. Conclusion

The purpose of this study was to examine the extent to which Stuxnet can be characterized as a new war, if at all. This has been of interest since defining the nature of Stuxnet is vital for both preparing and protecting ourselves from future destructive cyber-attacks. The material used in this study has been collected through a variety of sources, such as statements from cyber-security experts and decision-makers, public sources and previous research. Although the objectivity of public sources can be discussed, I believe that the wide range of varied material has contributed to a perhaps more nuanced description of the case than it would have if one merely used one certain sort of data. The empirical analysis has then been divided into three sections, where each part focuses on different aspects of the attack within the theoretical framework of new and old wars. The first section of the empirical analysis conducted that the aim of Stuxnet was political and highlighted the absence of both the private (criminal objectives) and political (ethnic, tribal or religious) purposes in new wars. The second part presented that the main actors involved in Stuxnet were nation states, including the attackers and the victim. This is again in accordance with the concept of ‘old wars’, that argues that wars entail merely nation state actors. Although states are believed to be involved in ‘new wars’, the theory argues that other actors, such as criminal organizations or non-governmental are part of the war as well. The third and final aspect, is discussing the method of Stuxnet. Stuxnet was implemented digitally and caused severe physical damages on the target, without the victim even realizing that it was under attack. This contradicts the concept of ‘old war’, which argues that the objective of war can only be applied through the use of force. Stuxnet did reach its goal in the sense that it sabotaged crucial parts of the Iranian nuclear program without using violence. In this regard, Stuxnet was conducted in accordance with the theory of ‘new wars’ that argues that violence is avoided and even unnecessary in new wars.

It is therefore evident to conclude that Stuxnet cannot be characterized as either an old nor new war, but rather a combination of both. In regard of the research question; Stuxnet can be characterized as a new war in the extent of the method of warfare and the globalized context that contributes to the interconnected world, which assisted in spreading the digital weapon through devices located in all over the globe.

8. Bibliography

Alvarez, Joshua. Stuxnet: The world's first cyber weapon. Center for International Security and Cooperation, Feb 3rd, 2015 http://cisac.fsi.stanford.edu/news/stuxnet (viewed 18th Apr)

Baylis, John., Smith, Steve., Owens, Patricia (red.). The Globalization of World Politics: An Introduction to International Relations. 4th edition. Oxford: Oxford University Press, 2008

Barret, James. Our Final Invention: Artificial Intelligence and the End of the Human Era, St. Martin's Griffin, 2015

Bryan, D. Stephen. Technology Security and National Power: Winners and Losers. Piscataway, NJ: Transaction Publishers, 2015

Bryman, Alan. Social research methods, Oxford University Press; 4th edition, 2012

Bryman, Alan., Bell, Emma. Business Research Methods, Published by Oxford University Press, 2010

Borger, Julian. The truth about Israel's secret nuclear arsenal. The Guardian, Jan 15th, 2014 https://www.theguardian.com/world/2014/jan/15/truth-israels-secret-nuclear-arsenal (viewed May 7th, 2017)

Cambridge Dictionary, "International community" http://dictionary.cambridge.org/dictionary/english/international-community (viewed May 10th, 2017)

Cordesman, Anthony H. Iran's Developing Military Capabilities, Centre for Strategic & International Studies, 2005

"Cybercrimes with Ben Hammersley". BBC News https://www.youtube.com/watch?v=4oNnSStrc38 (viewed May 13th, 2017)

David, Matthew., Sutton, Carole. Social Research: An Introduction, Sage Publications Ltd; 2nd edition, 2011

Deep, Alex. Hybrid War: Old concept, New Techniques, Small War Journal, Mar 2nd, 2015 http://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques (viewed May 11th, 2017)

Dehghan, Saeed Kamali. Iran accuses Siemens of helping launch Stuxnet cyber-attack. The Guardian, Apr 17th, 2011 https://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack (viewed Mat 14th, 2017)

Denning, E. Dorothy. Stuxnet: What has changed? Future Internet 2012, *4*(3), 672-687; doi:10.3390/fi4030672

Dodge, C. Ronald., Futcher, Lynn (Ed.). Information Assurance and Security Education and Training, Springer-Verlag Berlin Heidelberg, 2013

Enbody, Richard., Aditya Sood. Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware, Syngress; 1 edition, 2014

Falkenrath, Richard. Bloomberg https://www.youtube.com/watch?v=VAXOTJkzGL8 (view May 13th, 2017)

Geers, Kenneth. Strategic Cyber Security, Kenneth Geers, 2011. ISBN

Gibney, Alex. The Secret Cyberwar is Here: Director Alex Gibney on 'Zero Days' Documentary, Stuxnet & Cyberweapons, (Online video), Reason, July 8th, 2016 http://reason.com/reasontv/2016/07/08/the-secret-cyberwar-is-here-director-ale (viewed May 18th, 2017)

Hafemeister, David. Nuclear Proliferation and Terrorism in the Post-9/11 World, Springer; 1st ed. 2016 edition, 2016

Hamel, Jacques., Dufour, Stephane., Fortin, Dominic. Case Study Methods (Qualitative Research Methods)", SAGE Publications, Inc;1 edition, 1993

Henderson, Errol., Singer, David. "New Wars" and Rumours of "New Wars", International Interactions: Empirical and Theoretical

Hoffman, Frank. Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies, 2011.

Jacques, Martin. "What the hell is the international community". The Guardian, Aug 24th, 2006 https://www.theguardian.com/commentisfree/2006/aug/24/whatthehellistheinternati (viewed May 12th, 2017)

Kaldor, Mary. New and Old Wars: Organized Violence in a Global Era. Stanford University Press; 3rd edition, 2013

Langer, Ralph. "Att knäcka Stuxnet, 2000-talets cybervapen". TED Talk, March 2011 https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon?language=sv (viewed May 18th, 2017)

Loukas, George. Cyber-Physical Attacks: A Growing Invisible Threat, Butterworth-Heinemann; 1 edition 2015

Maclean, William. Nov 16th, 2010, Reuters *"Stuxnet study suggests Iran enrichment aim: experts"* http://www.reuters.com/article/security-cyber-stuxnet-idUSLDE6AF0FX20101116 (viewed May 5th, 2017)

Micallef, Joseph V. The other bomb: Pakistan's Dangerous Nuclear Strategy. The Huffington Post, Jul 2nd, 2016. http://www.huffingtonpost.com/joseph-v-micallef/the-other-bomb-pakistans_b_9180504.html (viewed 7th May 2017)

Münkler, Herfried. The New Wars. Polity; 1 edition, 2004

Nachenberg, Carey, How a computer virus foiled Iran's nuclear program, CISAC Science Seminar, Apr 23rd, 2012. https://www.youtube.com/watch?v=DDH4m6M-ZIU (viewed May 18th, 2017)

North Korea's nuclear programme: How advanced is it?. BBC News, Jan 6th, 2017

http://www.bbc.com/news/world-asia-pacific-11813699 (viewed May 7th, 2017)

Nye, Joseph S. "The Power to Lead", Offord University Press, Inc. 2008

Poellinger, Clemens. Stort publiktryck på Chomsky-föreläsning. Svenska Dagbladet, Sep 20th, 2002, https://www.svd.se/stort-publiktryck-pa-chomsky-forelasning (viewed May 10th, 2017)

Remarks by Secretary Panetta on Cybersecurity and Business Executives of National Security. Department of Defense, New York, U.S. Oct 11th, 2012 http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136 (view May 13th, 2017)

Richard A. Clarke, The Economist's World in 2013 Festival, Dec 8th, 2012, https://www.youtube.com/watch?v=6_ek8mugOUc (viewed May 13th, 2017)

Rosenzweig, Paul. Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare, The Great Courses, 2013

Sanger, David E. Obama ordered wave of cyberattacks against Iran, The New York Times, Jun 1st , 2012 http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (viewed May 13th, 2017)

Schreier, Margrit. Qualitative Content Analysis in Practice, SAGE Publications Ltd; 1 edition, 2012

Secretary- General Examines 'meaning of international community' in address to DRP/NGO Conference, 15th Sep 1999, http://www.un.org/press/en/1999/19990915.sgsm7133.doc.html (viewed May 12th, 2017)

Shackelford, Scott J. Managing Cyber Attacks in International Law, Business, and Relations: In search for Cyber Space. Kelley School of Business, Indiana University 2014

Simpson, Emile. War from the Ground Up: Twenty-first Century Combat as Politics, Oxford University Press; 1 edition, 2012

Sood, Aditya., Enbody, Richard, Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware, Syngress; 1 edition, 2014.

Taddeo, Mariarosaria, Glorioso, Ludovica (Eds.). Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative, Springer International Publishing, 2017

The Middle East: Abstracts and index. Library Information and Research Service, Northumberland Press 2006, University of Michigan.

Volz, Dustin., Finkle, Jim. U.S. indicts Iranians for hacking dozens of banks, New York dam. Reuters, Mar 25th, 2016
http://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WQ1JF (viewed May 13rd 2017)

What is a Zero-Day Vulnerability?, PC tools by Symantec,
http://www.pctools.com/security-news/zero-day-vulnerability/ (Viewed May 16th, 2017)

Williams, John. The Ethics of Territorial Borders: Drawing Lines in the Shifting Sand, Palgrave Macmillan; 1st ed. 2006

Wired https://www.wired.com/author/kimzetter/ (viewed 26th Apr 2017)

Zorz, Zeljka. Israeli general claims Stuxnet attacks as one of his successes. Help Net Security, Feb 15th, 2011
https://www.helpnetsecurity.com/2011/02/15/israeli-general-claims-stuxnet-attacks-as-one-of-his-successes/ (view May 13th, 2017)

60 Minutes, "Stuxnet: Computer Worm Opens New Era of Warfare”
http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/
(viewed Apr 1st, 2017)

(2011) Stuxnet: targeting Iran's nuclear programme. Strategic Comments, 17:2,1-3, DOI: 10.1080/13567888.2011.575612