UPPSALA
UNIVERSITET

Gendering Cyber Warfare

A theoretical and exploratory paper addressing the research gap on the gendered aspects of cyber warfare

Mahlet Abera Techan

Under the supervision of:

Maria Eriksson Baaz

Department of Government

Spring 2020

30 Credits

Abstract

War is gendered. The scholarship of gender and war is comprehensive and multi-layered, yet there seems to be some difficulty to keep up with the new developments in technology and its involvement in warfare. It was only until a few years ago that a new method of warfare - cyber warfare, a form of hybrid warfare, emerged and got the spotlight in the discussions on new methods of warfare. However, as the literature is growing, and international organisations are producing policy and strategy documents on cyber warfare, there seems to be a research gap on the relation between gender and cyber warfare, more specifically the gendered aspects of cyber warfare. This thesis attempts to fill that research gap and intends to answer how cyber warfare may be gendered. This is be done by generally looking at the literature of "Gender and War" and "Gender and Cyber", and Gunneriusson and Ottis (2013) categorisation of how cyberspace is used in military operations from a hybrid warfare perspective. Gunneriusson and Otitis's categorisation focus on inter alia cyber-attacks on non-military targets, and the use of propaganda. The overview of the research on gender and cyber focus on the workforce within cyber related sectors and gender-based violence, and the overview of research on gender and war brings up numerous examples of the nexus between gender and war. Based on the overview of the two fields of research along with Gunneriusson and Ottis categorisation this thesis comes to the conclusion that cyber warfare can be gendered. The purpose of the examples of cyber-attacks are the same when same attacks are conducted offline and these types of attack offline have the same effect online. The difference is that an attack through the cyberspace intensifies the consequences in comparison to when these same methods were used in other domains.

Key words: gender, cyber warfare, hybrid warfare

Table of Contents

1. Introduction

We are exposed to gendered imaginings of war every day whether it is a fairy-tale story about a prince saving a princess, or a Hollywood film about brave western men fighting the big wars while their loved ones are back home, or videos of crying women and children from a warzone spreading on social media (Sjoberg, 2014; Welland, 2018). These platforms, (books, films, social media) present gendered imaginations of war and most often portray women and med based on traditional stereotypes and assumptions where the man is seen as the stronger sex and the protector of the supposedly vulnerable and the weak – the woman. These traditional stereotypes portray women as caregivers, nurses or as innocent civilians who are in need of protection (Goldstein, 2006). These traditional stereotypes are based on social constructions that have created gender ideals for women and men. The examples of a heroic prince, brave soldiers and crying women and children indicate that to go war is justified when the reasoning is to "protect women from our enemies" (Goldstein, 2006).

This justification implies that war is gendered. That women and men are affected by war(s) differently is recognised internationally and clearly expressed in the United Nations Security Council Resolutions, e.g. 1325 and 1820, and in the emergence of the Women, Peace and Security Agenda (Sjoberg, 2014). Moreover, the nexus between gender and war has received much attention in academia and the public debate (Baaz & Stern, 2011; Bjarnegård et al. 2015). Within the literature of war and warfare the focus has until recently concerned conventional traditional warfare, where the aim is to defeat the opponents' military forces in order to influence the opponents' government (Hasler, 2007). Interestingly, with the development of technology and recent events in Ukraine, the spotlight has turned to the concept "hybrid warfare" (Hoffman, 2018). Hybrid warfare entails in general terms, a combination, a hybrid, of conventional and unconventional warfare. Unconventional warfare is not the opposite of conventional warfare and as the definition evolves the core tenants of unconventional warfare entail warfare where the operations are conducted by, with or through irregular forces (Hasler, 2007). The term hybrid warfare is used by both state and non-state actors and has become a prioritised preoccupation for international organisations such as the European Union (EU) and North Atlantic Treaty Organisation (NATO) (Giegerich, 2016).

Hybrid warfare is a rather abstract term and there is no agreed definition. An example of conventional warfare that is used together with unconventional warfare is information warfare. As will be further explained below, there are different forms of information warfare and one of the most popular discussed form is cyber warfare (Heickerö,2010). In most literature, cyber warfare includes everything from cyber-attacks to propaganda (Libicki, 1995). While the use of propaganda in wars and conflicts is not a new phenomenon, the development of information and communication technology (ICT) provides new venues, and much propaganda is found online and especially on social media platforms (Gunneriusson & Ottis, 2013). The emergence of cyber-attacks is also a consequence of the development of technology (Winterfeld & Andress, 2013). In brief, this new development in warfare concerning strategy and method is the emergence of a new field, cyberspace.

Gender and War literature focuses on the nexus between gender and war and presents a more comprehensive understanding of the dynamics of war since gender roles are central to apprehend the complexity of wars and conflicts (Bjarnegård et al. 2015). Therefore, it is vital for gender and war literature and international organisations to keep up with the "new" developments especially the use of cyberspace and emergence of cyber warfare and examine and analyse how it is gendered. Interestingly, the EU and NATO have released several policies and reports, and even established a centre which focuses on hybrid threats and warfare, yet, a gender perspective is more or less missing according to Charlotte Isaksson (personal communication, 24 September 2019). Even more interestingly, a gender perspective on this conduct of war seems to be missing as well within gender and war scholarly literature. While the research on the use of cyber warfare is expanding rapidly, there is barely any discussion on the gendered aspects of this warfare.

This thesis is a modest attempt to fill this research gap. Originally the idea was to analyse how major international actors – mainly EU and NATO – apply gender to hybrid warfare and the gendered assumptions underlying this. Yet, while searching for documents and after consulting with a gender expert, C. Isaksson (personal communication, 24 September 2019), who is highly placed both at EU and NATO, it turned out, as already concluded above, that gender perspectives is more or less still missing. In short, major international and organizations, as well as research, have not yet really addressed the

question: How may cyber warfare be gendered? Asking that question is crucial. Without the gender aspect, it is difficult to understand the levels of complexities of war and conflicts (Bjarnegård et. al 2015).

1.2 Aim

The main purpose of this thesis is to make a first and theoretical attempt to fill the gap in knowledge on how cyber warfare may be gendered. This will be done by drawing upon literature within three main, and largely separate, fields of research: namely "Cyber warfare", "Gender and War" and "Gender and Cyber". Thus, the main research question is: what can the literature within the "Gender and War" and "Gender and Cyber" fields teach us about how cyber warfare may be gendered? The analysis in this thesis will be conducted in four steps and is guided by the following questions:

1. What is cyber warfare and how does that form part of the concept of hybrid warfare?
2. What does the general literature on Gender and War tell us about how war is gendered?
3. What does the general literature on Gender and Cyber tell us about how cyberspace is gendered?
4. Drawing upon the concept of cyber warfare and its various dimensions (identified in the first question) and the literature on Gender and War as well as Gender and Cyber. How may cyber warfare be gendered?

1.3 Previous Research and Original Contribution

As explained above, this thesis draws upon and contributes literature within three main and largely separate, fields of research, namely "Cyber warfare", "Gender and War", and "Gender and Cyber". As these fields will be elaborated on later in the thesis I will in this section give some general information about the fields, and some of the central topics.

As explained briefly above, the emergence of hybrid warfare has been discussed generally academically and professionally, and two of the main issues discussed are whether hybrid warfare is a new method of warfare and the growing use of cyberspace and the extensive consequences (Frideman, 2019). There are two schools of thought concerning the

emergence of hybrid warfare (Johnson, 2017). According to Frank Hoffman, who is considered by many scholars the first leading scholar to discuss the understanding of the concept contemporary warfare and specifically hybrid warfare, claims that hybrid warfare is indeed not new, but it is different from previous methods of warfare (Hoffman, 2009). This is the opinion of the first school which argues that it is a useful concept, but that is not enough of a reason for it to be considered new. The second school of thought is more open minded and provides several definitions of what hybrid warfare entails and includes normally the categorization 'asymmetric warfare' which is a combination of conventional and unconventional warfare focusing on the "operational reach of terrorism" that uses new technology (Johnson, 2018). Taking into account that the second school of thought is more varied, there is still an agreed idea that hybrid warfare is a new conduct of war and thereby a need to produce new strategies (Johnson, 2018). Furthermore, in 1993 John Arquilla and David Ronfeldt warned for the advancement of technology and how it would enable conduct of war to develop. At the time it was not received with much attention. Fast forward to the 21st century, Arquilla and Ronfeldt were correct, and the development of technology within warfare is still a blurry issue and has created many challenges for states, companies and organizations (Arquilla & Ronfeldt, 1993).Commonly, cyberspace is referred to as the fifth battlespace, after land, air, sea and space (Cornish, Livingston, Clemente, & York, 2010). Technology has made cyberspace not only a new fifth field but also increased the speed for threats to evolve and has given disproportionate power to smaller actors (Cornish, Livingston, Clemente, & York, 2010). This cyber dimension is not necessarily a new categorization but instead an "improved tool of warfare" (Bachman & Gunneriusson, 2015 p.83).

The thesis naturally also links to and contributes to the scholarship of gender and war which is wide and covers more varied themes in comparison to the cyber warfare discourse. A fundamental idea in gender and war theory is that gender is "co-constitutive" meaning gender is used to legitimize wars and due to gender ideals and roles the effects of war(s) are different between women and men (Enloe,2000). Some of the most leading scholars in gender and war literature and research are inter alia Jean Bethke Elshtain, Cynthia Enloe, Joshua S. Goldstein and Laura Sjoberg. While some scholars address both aspects of the ways in which gender and war is co-constitutive e.g. Enloe and Goldstein, some focus mainly on one aspect. Hence, some scholars focus on how gender is used to legitimize wars, and others focus on how war affects women and men differently,

highlighting how women's experiences and contributions have been silenced (Goldstein, 2006). Examples of such scholarship are research on women in military organizations as soldiers, combatants and in various supporting functions and research on conflict related sexual and gender-based violence. Nevertheless, these examples of fields of research in the scholarship of gender and war barely take into account the use of cyber warfare.

The third field is Gender and Cyber, this is a rather new field were the focus is not much on the conduct of war but instead on the workplace, such as the cyber security industry, and the the lack of women working with cybersecurity (Peacock and Irons,2017). The common argument is that cyberspace is gender neutral, nonetheless, the workforce in cyber security and other cyber-related workplaces are primarily male dominated. (Kramarae & Spender,2000). Another central issue in the Gender and Cyber field is how cyberspace is enhancing gender-based violence online (Suzor et al. 2018). Gender-based violence is not new phenomenon, and with the development of technology and the emergence of numerous social media platforms, gender-based violence is found both offline and online. Gender-based violence is used aa a weapon of war and now cyberspace has become a facilitator for gender-based violence online which has led to new problems arising.

As mentioned above, the nexus of gender and hybrid warfare and cyber warfare barely exist and the original idea for this paper was to analyse the EU and NATO and their policies and strategies on how they combat hybrid threats that are cyber related and examine how they include a gender perspective. Since there is lack of research on the issue, the purpose of this paper hence changed to exploring theoretically, based on the findings from the fields, how cyber warfare may be gendered. Therefore, this paper seeks to make an attempt to help fill the knowledge gap, and through examining the literature of Gender and War and Gender and Cyber and apply it to the literature of cyber warfare. This is done to facilitate the application of the two research fields. Also, this paper is grounded on the idea on gender as co-constitutive. Lastly, it is also necessary to take into account that this is a first attempt to examine the nexus of gender and cyber warfare, and thereby this paper is will be more of an overview.

1.4 Limitations

It is important to take into account that this paper is a first attempt to investigate a nexus that is barely discussed. Therefore, it is important to keep in mind that the aim of this paper is not to make a claim on how cyber warfare is gendered. This would also be impossible given that the ways in which is gendered will always depend on context (Goldstein, 2006). This thesis will rather highlight some possible ways in which it might be gendered and contribute with questions that we may need to ask in forthcoming efforts. Moreover, given that the fields, "Cyber warfare", and in particular "Gender and War", and "Gender and Cyber" are huge and multi-layered fields this paper is not claiming to cover the whole field but rather make use of the fields in broad terms. In addition, the thesis results are of course also, by necessity, based on a particular definition of hybrid warfare and cyber warfare (to be described further below). Hence, with another definition one might arrive at other conclusions and other perspectives would be highlighted more than it is in this paper.

2. Research Design, Material and Structure of Analysis

As explained above, this is a theoretical and exploratory paper addressing the research question: what can the literature within the "Gender and War" and "Gender and Cyber" fields teach us about how cyber warfare may be gendered? The paper will follow the order of the guiding question, which is presented in 1.2 Aim. Consequently, there are some more detailed sub-questions and steps:

1. What is cyber warfare and how does that form part of the concept of hybrid warfare?
    a. How is hybrid and particularly cyber warfare defined in the literature?
    b. What aspects of warfare does it entail?
    c. How does these forms differ from conventional warfare?

This part, question 1, will end with a conceptualization which will later provide the basis of the analysis.

2. What does the general literature on Gender and War tell us about how war is gendered?
    a. In what ways does gender facilitate war?
    b. How does war affect women and men differently and why does this happen?

3. What does the general literature on gender and cyber tell us about how cyber is gendered?
4. Drawing upon the chosen concept of cyber warfare and its various dimensions (identified in the first question) and the literature on gender and war as well as gender and cyber, and drawing upon the idea of war and gender as co-constitutive in the gender and war literature, produces the following questions
    a. In what ways may gender and cyber be used in facilitating warfare?
    b. How might cyber warfare affect women and men and the roles they play in war differently?

Since this paper is a first theoretical attempt, the discussed literature and scholarship will be from mainly leading scholars in the respective discourse. The leading scholars are normally most cited and referred to, and the scholars mentioned in the previous research section are some example of the leading figures. In addition, besides literature from the leading and most cited scholars, much of the material concerning hybrid warfare and cyber warfare will be material that has been published only in the recent years since this discourse is rather new and is a rapidly growing field. Moreover, there is an ongoing debate on the distinction between the scholarship on hybrid warfare and cyber warfare in the Global North and South (particularly the East). It has become common that scholars from the Global North and South criticize and compare each other works and especially concerning the approach of defining the relevant concepts or how non-state actors use of information warfare such as cyber warfare (Fridman, Kabernik & Pearce, 2019). This has been taken into consideration and has not been a determinant factor in the researching phase. Nonetheless, the paper will not go further into this debate hence the paper is focused main on research from Global North since it is a dominating perspective. Additionally, the focus of this paper is not on defining the concepts or the role or non-state actors hence this should not be an issue.

2.1 Structure of analysis

The four guiding questions and sub-questions form the outline of this paper. It starts with three chapters covering the literature and scholarship of first Hybrid warfare and Cyber warfare, secondly Gender and War, and lastly Gender and Cyber. The first chapter will explain the hybridity and the relation to cyber warfare, along with an overview of cyber warfare, and how it is conceptualized and the role of propaganda. The second chapter,

Gender and War, is formed based on the idea that gender is co-constitutive and will include several empirical examples. The third chapter will focus on the debate on cyberspace as the workplace is male-dominated, followed with a section focusing on gender-based violence online. Next will be the analysis with the aim of answering the fourth guiding question and its sub-questions. That chapter is structured around the conceptualization of cyber warfare and the theoretical and empirical conclusions from the previous three chapters. The paper will finish with a conclusion answering the main research question.

3.General Overview on Hybrid Warfare & Cyber Warfare

The attention on hybrid warfare and hybrid threats quickly rose in 2014 with Russia's annexation of Crimea when the so-called little green men, wearing unmarked green uniforms and carrying Russian weapons, entered the territory (Hoffman, 2018). Hybrid warfare might not be a new phenomenon since there is no agreement concerning the definition of hybrid warfare and whether hybrid warfare is a new method of warfare or just a new label. In the introduction chapter, the current debate on the issue of how to approach the definition was briefly explained and what hybrid warfare and cyber warfare entail. Therefore, this chapter will explain in what way cyber warfare forms part of hybrid warfare. Firstly, there is a recap of what hybrid warfare is, and then secondly a more extensive description on cyber warfare will be given – what it entails and what forms exist, and the last section will cover how cyber warfare can be conceptualized and how propaganda is part of this conceptualization.

3.1 Recap Hybrid warfare

Hybrid warfare has several names such as special warfare, ambiguous warfare and grey operations (Johnson, 2018). The common distinction of warfare is between conventional and unconventional or irregular warfare. Yet, it is not easy to make a distinction between these three which makes it more difficult to agree on a definition for hybrid warfare. At this moment there is no contemporary hybrid warfare definition, scholars, military personnel and larger international organizations such as EU and NATO have not agreed on a united interpretation of hybrid warfare. Scholar Bastian Giegerich (2016) explains that the increased attention on hybrid warfare is only due to it being trendy but that it is not something new. It is simply a modern-day interpretation of the combination of conventional and irregular combat (Giegerich, 2016). On the other hand, Giegerich

explains that the opponent's arguments for hybrid warfare being new is because it "has become a convenient label to file away all the issue we currently do not understand about changing character of conflict" (Giegerich, 2016, p.67). Moreover, scholar James K. Wither (2016) argues hybrid warfare is more new than old. He claims that the term is used to name contemporary warfare that is characterized by increasing violence from non-state actors and growing use of cyber warfare. The reason for it to be considered more new than old is the combination of conventional and irregular warfare is not seen in the same way as in the past.

Furthermore, within the literature on this rather 'new' topic, Hoffman's definition is continuously used. According to Hoffman, both non-state actors and states can use hybrid warfare and define hybrid warfare as: "incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts, including indiscriminate violence and coercion, and criminal disorder" (Hoffman, 2007, p.14). He also explains that hybrid wars "blend the lethality of state conflict with the fanatical and protracted fervour of irregular warfare… the term capture both their organization and their means" (Hoffman, 2007, p.28). With that said, since this issue has been discussed already at the time of Chinese general Sun Tzu in late sixth century BC, and that Hoffman's presentation of hybrid warfare is continuously referred to, this thesis will use his definition as well.

The traditional approach to characterise warfare is to differentiate between conventional and unconventional warfare, and commonly, wars and conflicts are using both conventional and unconventional warfare, also referred to as compound wars (Hoffman, 2007). For instance, during the Rwanda genocide radio and print media were used for propaganda in addition to the massacre, or in the battle of Hezbollah against the Israel Defence Force in Lebanon in 2006, Hezbollah used a combination of "militia units, special trained fighters, and the anti-tank guided- missile teams" (Hoffman, 2009, p.37), and new media audiences to influence public opinion and more (Goldstein, 2006). However, it was in 2014, with Russia's annexation of Crimea where the so-called green men entered Crimea, that the concept of hybrid warfare received more attention (Hoffman, 2018). Green soldiers with no marked uniforms entered Crimea, no-one confirmed who they were or why they were there, and propaganda campaigns were launched (Schnaufer, 2017). Since then the concept has been on the radar in the discussion

on modern warfare (Reno, 2018). This does not mean that the warfare used in the 21st century is replacing traditional or conventional warfare but illustrates the increased complexity for defence planning (Hoffman, 2007).

In order to understand the concept of hybridity, David Betz (2019) has presented some characteristics on the hybridity of warfare, in a book released only a few months before this paper was finalised. The first characteristic is that the easy categorisation of conduct of war does not hold anymore as it has become blurred since non-state actors can have "capabilities and organisation that are state-like"(Betz, 2019, p. 9) and state actors can use methods that are regarded as guerrilla-like. State and non-state actors do this in order e.g. to avoid legal restrictions or that there will be quickly escalating consequences if they did it in a conventional way (Betz, 2019). The second characteristic that makes it hybrid is that there is a mixture of conventional and unconventional "tactics and means which is employed to sustain the hybrid force, to facilitate the disruption of the target nation and protract the conflict" (Betz, 2019, p. 10) Nonetheless, the new addition to the conduct of compound wars is the development of information technology and its new role in contemporary warfare (Betz, 2019, p. 14). The main development of information technology is the creation of cyberspace which has consequently led to the formation of cyber warfare. When the little green men invaded Ukraine in 2014, the attention on hybrid warfare was focusing on how cyberspace was used in form of cyber warfare and propaganda (Caliskan & Cramers, 2018). The use of cyberspace and specifically cyber warfare has become an added concept to discuss when discussing hybrid warfare. The following section will look deeper into this new arena, cyberspace, what it entails and how it can be conceptualised.

3.2 Cyber Warfare

The terms cyber warfare and information warfare are used interchangeably. Although there are some major differences, and in most states, cyber warfare is a branch of information warfare (Jones & Kovacich, 2016). There is no agreed definition of cyber warfare, though the UN Interregional Crime and Justice Research Institute defines cyber warfare as "…any action by a nation-state to penetrate another state's computer networks for the purpose of causing some sort of damage. However, broader definitions claim that cyberwarfare also includes acts of 'cyberhooliganism', cybervandalism or cyberterrorism" (Jones & Kovacich, 2016, p. 42). In other words, it is warfare conducted

in cyberspace. Cyberspace can be defined as a" globally interconnected network of digital information and communications infrastructures, including the Internet, telecommunications networks, computer systems and the information resident therein" (Melzer, 2011, p. 4).

Today cyberspace is militarized and intensified and is used both on a "tactical, strategical and operational level (Bachman & Gunneriusson, 2015, p. 83). The international organizations, e.g. EU and NATO are continuously producing documents and releasing policies on cyber warfare[1] and states such as the United Kingdom (UK), and the United States of America (US are taking this issue seriously and have produced numerous strategies (Cornish, Livingston, Clemente, & York, 2010).

The purpose to conduct cyber warfare is the same as for conducting conventional warfare, the difference between these two is the means and not the ends (Chen & Dienrman, 2016). The wish is to protect ICTs and its gathered intelligence, and consists of "software, hardware, and firmware"(Chen & Dinerman, 2016, p. 53) The conduct of cyber warfare entails launching cyber-attacks, which are mostly "opaque and in stealth mode" (Chen & Dinerman, 2016, p. 54). It is difficult to determine who launched the attack, since both state actors and non-state actors use this method of warfare. The targets are commonly critical information infrastructures such as hospitals, banks, and media outlets. One might believe this indicates that there is no physical damage but that is not always the case. Nevertheless, the damage is still grand as cyber-attacks can cause massive information loss (Chen & Dinerman, 2016). In comparison to conventional warfare, is cyber warfare not declared. Cyber warfare is an ongoing process and the attack itself usually occurs during a short period of time (Chen & Dinerman, 2016).

[1] See for example: Joint communication to the European parliament, the European council and the council Increasing resilience and bolstering capabilities to address hybrid threats (JOIN/2018/16 final) and The NATO Cooperative Cyber Defence Centre of excellence (https://ccdcoe.org/).

3.2.1 Categorisation of cyberspace

As explained above, cyber warfare is a branch of information warfare, and cyber warfare is warfare conducted on cyberspace. Håkan Gunneriusson and Rain Ottis (2013) wrote an article on the cyber dimension from a hybrid warfare perspective, with a focus on the military community. They suggest three ways to categorise how cyberspace is used in military operations. The first approach is using cyber warfare as a support to the conventional forces. This entails a combination of conventional warfare and cyber operations e.g. cyber-attacks. Other examples of this approach are drones and guided missiles or attacks on control and logistics systems (Gunneriusson & Ottis, 2013). These operations aim is to cause disruption on control systems, logistics and communication systems or to disrupt an airstrike or to disrupt a drone such as the event in 2011 when Iran managed to prevent a US drone to land in Iran (Gunneriusson & Ottis, 2013). The second approach is attacking non-military targets, which in other words mean cyber-attacks on systems that are not associated with the military. The difference from the previous example is that attacks on non-military targets are not the responsibility of the military to protect. Non-military targets are commonly critical information systems (CIIs) whose purpose is to "maintain our way of life" e.g. banks, hospitals, water plants and power plants. Hence, attacks on these CIIs can cause physical harm. However, there are no existing examples of this, nonetheless, cyber-attacks on non-military targets can cause great harm such as disruption in a bank system or on hospitals IT-systems harming both patients as well as the personnel. Lastly, the third approach is focusing on "exploring the opportunities provided by this environment" (Gunneriusson & Ottis, 2013, p. 103). Gunneriusson and Ottis explain that cyberspace "has offered ways to accomplish task that were previously prohibitively expensive or complicated" (Gunneriusson & Ottis, 2013, p. 103). For example, after the coup d'état in Turkey in 2016, access to the internet was limited as a consequence of the unrest that had emerged. Another example is that today state actors, as well as non-state actors, can spread propaganda and recruit people all over the world, share material, gather intelligence and plan and coordinate attacks to much greater extent than before (Gunneriusson & Ottis, 2013). In this field the actor is not necessarily military, however, it is known that criminal groups and terrorist organisations use cyberspace to facilitate their actions which then becomes an issue from a national security perspective (Gunneriusson & Ottis, 2013). Gunneriusson and Ottis put more emphasis on information warfare, such as forms of propaganda, on cyberspace in this third approach and that is not limited to be used by non-state actors. As the new field,

cyberspace has expanded the reach, since people can connect with each other through just a phone or a computer, and information spreads faster than ever and through numerous media platforms. As a consequence of the quick spread of information, examples of "fake news" and misinformation as well as propaganda have become more visible (Habgood-Coote, 2019). Furthermore, Gunneriusson and Ottis categorisation of how cyberspace from a hybrid warfare perspective, is not the only option. Their categorisation puts emphasis on how warfare in only cyberspace can be used and not the different technical terms and types which is commonly done in research (Jones & Kovacich, 2016; Winterfeld & Andress 2013).

3.2.2 Propaganda in cyberspace

Propaganda is clearly not a new phenomenon. Propaganda and psyops can easily be used interchangeably, the difference is however that propaganda is "the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behaviour to achieve a response that furthers the desired intent of the propagandist" (Jowett & O'Donnell, 2006, p. 7). While psychological operations (psyops) "seeks to convey selected information to target audiences to influence their behaviour and, through them, government policy" (Macdonald, 2007. p. 32).

Furthermore, cyberspace has become an important channel to spread propaganda and there are new alternatives to approach propaganda, for example, Jason Stanley (2015), who has taken on a bit of different approach than the traditional methods. Stanley claims propaganda can be categorised in two ways: supporting and undermining propaganda. Supporting propaganda is, for example, using a country's flag or romanticising a state's history in order to strengthen patriotism. This sort of propaganda aim is to "increase the realisation of a political ideal…by promoting an ideal and not by providing reasons or rational arguments for that ideal, but by emotional or other non-rational means" (Stanley, 2015, p. 53). He defines supporting propaganda as: "A contribution to public discourse that is presented as an embodiment of certain ideals yet is of a kind that tends to increase the realisation of those very ideals by either emotional or other non-rational means"(Stanley, 2015, p.53).

The second way of categorising propaganda, undermining propaganda is defined by Stanley as "a contribution to public discourse that is presented as an embodiment of certain political ideals, but is of a kind that tends to erode those a political ideal that belongs in the same family"(Stanley, 2015, p.54). The purpose is "an embodiment of an ideal, but which in fact tends to undermine the ideal it is meant to be in service of"(Stanley, 2015, p.54). In other words, it "references an ideal but do so by undermining those actual ideals" (Stanley, 2015, p.53-54). This categorisation is a bit difficult to understand in comparison to supporting propaganda. Stanley acknowledges the confusion and provides several examples. One example that clarifies the concept is the example of when Jews were portrayed as public health threat in the National Socialist Press in Germany. During Hitler's ruling, a statement concerning a public health was released in Germany. The public health statement claimed that Jews were a public health threat and they were compared to the Black Death. Since it was related to public health it was reasonable for many Germans to listen to. In addition, the people who believed in the anti-Semitic ideology trusted this statement. Yet, most Germans were Jews, meaning that this public threat statement was inconsistent with the health of this group. In other words, the content of the statement of Jews being a public threat is inconsistent with the actual purpose of releasing public health threat. It was for the Nazis benefits as they wish to "undermine" the Germans' view of Jews (Stanley, 2015).

To summarise, hybridity entails a combination of conventional and unconventional warfare, and information warfare is an example of unconventional warfare. In contemporary warfare cyberspace has become a central element and has thereby created a new conduct of war, cyber warfare. In other words, cyber warfare is a branch of information warfare and information warfare is an example of hybrid warfare. The purpose of cyberattacks is to hit CIIs and systems mainly relevant to a military. The damages can vary and do not necessarily have to be physical; it still causes great damages. To conceptualise cyber warfare is somewhat difficult but Gunneriusson and Ottis suggested an approach to conceptualise how cyberspace is used in terms of hybrid warfare: to complement the conventional warfare, to attack non-military targets and that cyberspace as an "environment" can be used to limit access to internet and thereby access to information or the use of propaganda. Next chapter will present the other untold main theme, beside cyber warfare, of this thesis, gender.

4. Scholarship of Gender and War

This chapter will revisit gender and war literature, and as stated in the introductory chapter, the central idea is that gender is co-constitutive. Gender as co-constitutive entails two things, first, that gender legitimises war abroad and at home, and secondly that women and men are affected differently from wars due to gender ideals and roles. Hence, this chapter is divided into two parts, starting with an overview of the main research on how men and women are portrayed in wars and how the attributes of these gender roles motivate humans to go to war. The second part will provide an overview of the main research on how women and men are affected differently from wars by examining the gender ideals, roles and responsibilities that are based on assumptions such as weakness and vulnerability. Clearly, much research cannot be divided into one of these areas of research as they have different dimensions (Goldstein, 2006). For instance, research on women's situation in the US during the Second World War shows how at first "home women" were recruited to enter the workforce, yet not long after the war has ended had the mindset changed and the glorification of women staying at home returned (Goldstein, 2006). Thus, this chapter will provide an overview and will not be able to discuss all different dimensions.

4.1 Gender as central in legitimising war at home and abroad

It is important to remember that gender ideals differ depending on the context and undergo changes (Goldstein, 2006). With that said, whether it is in films, books, or in media, research, particularly in the global North, shows that there is a common way to portray women and men. It is based on what is typically expected from women and men in war. Women are considered "beautiful souls" and men are seen as "just warriors", and that they, men, have the duty to protect the women since they do not participate in war(s) (Ehlstain, 1982; Sjoberg, 2014; Welland, 2018). Thereby, being portrayed as in need of protection indicates that women are weaker and vulnerable than their opposite sex, and unable to protect themselves (Sjoberg, 2014). Despite the fact that women have fought alongside men for centuries, women are still viewed as "helpless civilians" (Sjoberg, 2014, p.28). Simultaneously, men are expected to be the protector and the warrior along with other attributes that are considered masculine (Goldstein,2006). It is imposed on men that manhood plus masculinity equal "good warriors" (Goldstein, 2006, p. 252).

4.1.1 In war and in preparation for war

While such ideas reflect gender norms and ideals also in peacetime, research shows how they gain particular importance in war and in war preparations. There are numerous examples of how states have used oversimplified gender ideals to motivate their citizens to support the war(s) and to motivate their male citizens to join the armed forces or for other similar reasons. As Enloe (2000) writes, in war men are expected to behave even more like men and women even more like women. This is, for instance, illustrated in research on militarized masculinity which highlights how the military has been construed as a place which turns boys to men who embody physical strength, endurance, and honourability (Enloe, 2000). These are central to the idea of manhood, which has been generally imposed universally in military institutions (Goldstein, 2006). It is shown that this is done by excluding women – both as an ideal and as bodies. Militarised masculinity is privileging men over women and makes a distinction between "military men and feminised society" (Enloe, 2004, p. 106). It is imposing warriors to negate any feminine traits they might have (Goldstein, 2006). This exclusion is also based on the idea of wishing to safeguard the attributes and ideas of masculinity and femininity, and by perpetuating these ideas is a fundamental factor in motivating male soldiers "to fight the war(s)". Henceforth, this preservation of ideas of femininity and masculinity sets a standard of what is considered being in a warzone masculine and being at home as feminine (Goldstein, 2006).

As such promoting these types of ideal masculinities has been central in the preparation of war. Moreover, research shows how a construction of "our men" as the ultimate embodiment of physical strength, endurance and honour and shaming men who refuse to participate. For instance, during the First World War, women were active in shaming men to go out and fight the wars. Several campaigns were organised, recruiting posters which told men that if they refused to join the military they would be rejected by their women and at the same time posters addressing young women telling them that the men who did not join the military "were not worthy their affections"(Goldstein, 2006, p. 272). Such representations stand in contrast to the representation of enemy men – as feminized (weak) or as particularly brutal. One example of this is when the British radio played German gang rapes to provoke during the first world war, or when leaflets were dropped off by Italians telling Austrian soldiers that "while they were fighting Italy, Russians would occupy their homes and rape their women..." (Goldstein, 2006, p. 369). Hence the

enemy man described as particularly brutal. Another way of feminising the enemy, instead of portraying them as brutal is portraying them as weak, for example by castrating prisoners, mainly men, after or before being killed which symbolised emasculation (Goldstein, 2006).

A similar process, yet different, is visible in relation to women. Again, as Enloe concluded, war requires that men are men and women are women. In short, this has meant that while women also in peace are constructed as weak, nurturing, peaceful and in need of protection, such gender ideas tend to also be strengthened in war and war preparations (Enloe, 2000; Goldstein, 2006). Historically women have been associated with supportive and nurturing roles, being the witness, the mother, "sweethearts" and nurses (Goldstein, 2006). Gender and war literature has shown that war is legitimised through the motivation of protecting the helpless and innocent: women and children (Carpenter, 2006). While in peacetime women tend to be treated as a separate category, in a war they are lumped together with children - as Cynthia Enloe phrase it "womenandchildren" (Enloe, 2004, p.25) – thus reinforcing women's need of protection.

Most often the women that are considered in need of protection are the home women. They have become the representation for the peaceful, the beautiful soul and everything that is good (Ehlstain, 1982). This partly originates from the dichotomy of life as a combatant and life at home in peace, making life at peacetime at home is feminised and participating in the war is masculinized (Goldstein, 2006). Henceforth, there is a need to protect women and children as well a need to fight for them. Yet, these imageries are also sometimes used in relation to the protection of the "other women" in order to legitimize interventions. The most recent and most researched example is the war in Afghanistan. The Bush administration used gender stereotypes as part of their strategy to justify their war on terror (Höglund, 2010). This was done both by mentioning women's conditions in Afghanistan in official and public statements, as well as media showing pictures of women and children in need of rescue (Höglund, 2010). The intention was to publicly emphasize that the innocent women and children, "the other", need to be rescued from the horrible brutalities, in order for people to support their intervention in Afghanistan. It was argued as one of the main reasons why the U.S military started a war on terror. This is all based on the assumption that women are in need of protection since they are viewed

as innocent civilians, and this is still a motivation for humans to participate and join the armed forces (Goldstein, 2006).

Moreover, at the same time as women are portrayed as the beautiful soul, peaceful, innocent human beings the illustration will quickly change the moment women engage or in some way are associated with warfare. Women are then "dehumanized through sexualization" (Gentry & Sjoberg, 2015,p. 45). If associated with war making women are portrayed and told to be prostitutes and unstable as war making is not appropriate for women. There is a sort of stigma of women joining the army, perhaps not as much today as it was during the world wars since it contradicted the traditional gender norms. A woman who has joined the army, was contradicting the image of a home woman, by being described as whores, unstable and drinking too much (Gentry & Sjoberg 44-45). Still today, women who are engaged in warfare are demonized to sexual objects (Gentry & Sjoberg, 2015). Likewise, during the Second World War, leaflets with pornographic images of women were dropped off to disturb the soldiers on the front line which then portrayed women as whores (Goldstein, 2006).

Additionally, it is important to underline that home women not only are portrayed as weak creatures in need of protection but change the following demands of war. Moreover, due to the labour shortages during the second world war, propaganda through advertisements in "home magazines" were produced which glorified "the war working woman" (Yesil, 2004, p. 104). The idea was that the women would temporarily take over the men's jobs, and after the war, women would go back to their "proper roles" (Goldstein, 2006; Yesil, 2004, p. 104).

In other words, by portraying women as home women, peaceful and men as the just warrior and the protector wars have through history been justified as well as motivating humans to join the armed forces. Nevertheless, from the examples mentioned it is clear that each situation is contextual, and that women and men are not always portrayed and treated the same way as the examples mentioned above.

4.2 War affects women and men differently

The previous section provided an overview of how gender and war research has shown both how people are portrayed within this sphere and how the oversimplified gender

stereotypes have created an illusion of protecting the innocent and civilians which is synonymous with women, and children, and has been used as an argument to motivate male citizens to join the armed forces. However, as research also shows, the notion of women as in need of and also deserving protection has often not been adhered to. This is identified as "the protection racket" (Sjoberg & Peet, 2011, p. 7) and examples of this will be further elaborated below. The illusion of women in need of protection creates the idea that a state provides security, and by both scaring their female citizens of what can happen and at the same time promising them that the state will protect them leads to the creation of an illusion of protection which subsequently contribute to the justification for states to start wars (Sjoberg & Peet, 2011). This section will focus on the second part of the idea that gender is co-constitutive - that war affects women and men differently. This is based on the gender ideals and norms explained in the previous section. The idea of women as civilians and innocent, and men as strong, dominant protectors have an effect on how women and men are treated during wars but have also an effect on gender roles and the workforce during a war.

4.2.1 In the division of labour

In regard to the workforce, the traditional gender ideals and norms shape the division of labour. The gendered images of war portray men as part of a military while women stay at home or a supporting role to the military but not as a combatant. Combatants are traditionally associated with men and more "peaceful" roles are associated with women In addition, women have been associated with supportive and nurturing roles, being the witness, the mother, "sweethearts" and nurses in wartime (Goldstein, 2006). In wartime, are these roles intensified, as men leave their daily work to join the military women are left with taking care of the rest which included the tasks that were expected from them to do as well as taking on cheap or unpaid jobs to maintain the economy of a state in wartime (Goldstein, 2006). Nonetheless, research has shown that these gendered imagery of women and men are not showing the full picture. Women have had combat roles but that has barely been talked about and hardly mentioned in the literature of gender and war since it would contradict the traditional distinction between a military man and a home woman (Goldstein, 2006).

Furthermore, gender roles and work responsibilities are affected during wars. Throughout the wars in the 20th century, the workforce in the armies and civilian workforce went through several changes. For example, as mentioned briefly in previous section, in order for men to be available to join the armies during the Second World War the workplaces that were normally male dominated, such as the war industries, opened up and recruited women (Goldstein, 2006). The openings were announced and advertised as an alternative for women to show support for their men that were out fighting in the war. However, even if the gender stereotypes were "challenged" during wartimes it was still clear that this setting was temporary (Goldstein, 2006).

Furthermore, after the second world war and the Cold War, there has been an increase in the number of peacekeeping missions. These missions are male dominated and consist of both police and militaries. Masculine values are highly respected and prioritised in these institutions (Karim & Henry, 2018). In these peacekeeping missions the combat perspective is not necessarily required, but instead the priority is to "monitor peace agreements, provide credible information to all parties, prevent incidents of unrest from escalating, and help rebuild domestic institutions and infrastructure" (Karim & Henry, 2018, p.397). The skills that are linked to armed forces are not valued in these missions, instead the valued skills are the ones that are associated with "observing peace, mediate," and work with civilian sectors and NGOs (Karim & Henry, 2018). One could argue that these skills are more feminine than masculine. In Karim and Henry's chapter statements from the UN concerning the "sex ratio" for peacekeeping missions was analysed and concluded that their arguments indicate that female peacekeepers can ensure a reduction of sexual misconduct believing women are less likely to commit these crimes. According to authors that conducted this analysis, the arguments from UN are supporting the gender stereotypes of women being suited for roles that are considered feminine, for example the female Indian formed police unit work was praised but only "the feminine work in community engagement, not for the work for which it is deployed: to protect the population "(Karim & Henry, 2018, p.400).

4.2.2 As victims of violence

In regard to victims of violence of war men and women, as civilians and participants in war, are affected differently. Much of the research in gender and war has argued that women are the main victims, as civilians, of war. This has been problematized by scholars such as Charli Carpenter who in her book argued that there is a gendered image of the innocent civilians and that women are directly victimised due to the idea of women being weak and vulnerable while in fact both women and men are victimised but in different ways. For example, civilian men and boys are more often victims of killings and forced recruitment. The latter is clearly related to gender norms and ideas that men and boys are natural warriors. These boys are commonly from a lower-class, and it can be argued that the forced recruitment is gender-based as young boys and men are targeted more than young girls and women due to the traditional gender roles and norms explained above (Carpenter, 2006). Young girls and women are also forcibly recruited and there is a tendency that they are forced to do tasks related to the traditional gender role women have, such as cooking and cleaning (Denov & Ricard-Guay, 2013). In addition, young girls and women experiences from being forcibly recruited differ from young boys and men, where girls and women are victimised for forced marriage, sexual slavery and sexual violence (Denov & Ricard-Guay, 2013).

Rape in war is an example of how women and men are affected differently as victims of violence of war and is an example of how gender is used to represent domination (Goldstein, 2006). There is the idea that one is masculine and dominant and the other, the opposite, is subordinate and feminine (Goldstein, 2006). The use of rape as a weapon of war is not a new phenomenon, and the reasons why it is used depends on the context as there are different motivations. Yet, a commonly shared idea is that rape is a humiliation for the male enemy since they are raping the enemy's valued property, their women, thus the enemy is considered weak for not being able to provide protection (Goldstein, 2006). It comes down to the gendered norms of women being vulnerable and weak and thereby raping the enemy is a way of indicating their strength over the enemies. Yet, recent research highlight how also men and boys are victims of sexual violence more than what has been acknowledged since it has been regarded as an example of torture but also because the view of manhood is not synonymous with victimhood, and particularly sexual violence (Goldstein, 2006). Men are supposed to be the protector and the dominant and not the vulnerable, weak and feminine, which are considered synonyms to victims of rape.

To summarize, as one can see there are plenty of areas within this field of research that can be further explained and analysed. Hence, this is only an overview of the main research on gender and war. The first section shows why the gender roles and the portrayal of women and men as the beautiful soul and just warrior encourages humans to support the preparation to go to war, but also why men are motivated to join the military in order to protect their or other women. The second part covered how men and women are affected differently and used examples concerning the division of labor and women and men being victims of violence. The several empirical examples mentioned show that war is indeed gendered and co-constitutive. The following chapter will continue on the gender perspective but concentrating on cyberspace in general and not specifically the use of cyberspace in warfare, and the reason why will be explained below.

5. General overview on Gender and Cyberspace

In chapter 3 on hybrid warfare and cyber warfare it became clear that the literature on cyber warfare and cyberspace is rather new and quickly growing. This chapter will look at what the general literature on gender and cyber has to say, since the research question not only concerns gender and cyber warfare but also the relationship between gender and cyberspace. The nexus of cyberspace and gender can be perhaps difficult to recognise. Much of the literature concerning the relationship discusses the workplace and especially the workplace in cyber security. In addition, much of the literature focuses on whether cyberspace and the workplace are gender neutral or not. There is also a debate on how cyberspace has enhanced gender-based violence online which has led to new problems that will be explained below. This chapter will look at these two issues a bit further starting with how gender equal the workplace within cybersecurity is and the cyberspace role in the civilian sphere, focusing on gender-based violence online.

5.1 Gender neutrality

There is a fairly mutual consensus that the use of cyberspace is more or less gender neutral, however, the workplace in cybersecurity and cyber warfare indicate that it is still a male dominated field. The reasons for this are many. One way of explaining this situation is that the use of technology and security are “coded masculine” (Kramarae & Spender,2000, p. 284). There is also the traditional belief that within security sector, physical strength, fight mode, protection behaviours are synonymous with masculine

behaviours(Peacock& Irons, 2017). Thus, it has become more difficult for women to get a foot in the workplace. According to a study from 2017, 11% of the global cybersecurity workforce is female, and the underrepresentation is approximately this low, with the only difference of few percentage points, in US and EU (Peacock& Irons, 2017). Examples of reasons to the underrepresentation of women in the workforce are based on the absence of "familial encouragement, early engagement, encouragement within schools, appropriate careered education, female role models" (Peacock& Irons, 2017, p.26).

Interestingly, there is also a large pay gap of 23%, according to a study in 2011 (Peacock & Irons, 2017, p.28). Hence, and there is a mutual understanding that there is a "critical need to embrace the female talent in the cybersecurity field" (Peacock & Irons, 2017, p.26). The supporting arguments to why "the female talent" are needed are divided. On the one hand, research shows that a diverse workforce is beneficial for productivity and will perform better than a male-only organisation (Peacock & Irons, 2017 p.29). One the other hand, there is a need for the female talent and their "different" attributes. However, there is no agreement or explanation on what these attributes are and whether the attributes are referring to biological or social constructed attributes (Peacock & Irons, 2017). Contrariwise, there are suggestions that a human's performance in the use of technology or security has nothing to do with whether the person is expressing masculine or feminine features (Peacock & Irons, 2017).

5.2 Gender-based violence online

Gender based violence is not new phenomenon and is widely and vividly discussed among scholars and in gender and war literature (Suzor et al. 2018). As the availability to internet has expanded and the use of social media as well as the different online platforms has unfortunately led to the phenomena of gender-based violence online (Rehrl, 2018). Gender based violence in conflicts is used to "attack, oppress and silence" a state (SIDA, 2019, p. 1). Studies show that both men and women are victims to the different forms of gender-based violence online, but girls and women are still in majority of being victims to it. Gender-based violence online can take form of harassments, stalking through apps, revenge pornography, images of sexual assaults, threats of rape and abuse. The development of technology, and the expansion of cyberspace has had positive effects in regard to freedom of speech but also negative effects as cyberspace have now

become a facilitator for gender-based violence (Suzor et. al 2018). As a facilitator it is "projecting, reproducing inequality and traditionalist stereotypes (Suzor et. al 2018).

Moreover, cases of online sexual violence and especially photos of sexual violence that are uploaded to cyberspace have been reported in media numerous times and the reactions has varied and a discussion on the reactions have emerged because of the tendency of blaming the victim (Dodge & Spencer, 2018). As women have been told to be whores and sluts for joining the armed forces, women that are victims of online sexual violence have been told the same (Dodge & Spencer, 2018). As images and videos of online sexual violence spread on social media platforms, the victim, especially if it is woman, is blamed because she "has asked for it" and therefore deserves it (Dodge & Spencer, 2018). In an article by Dodge (2016), is Judith Butler's concept "digitalising the evil" used to explain the blaming and they conclude that "that rape culture, and the myths that enforce it such as stereotypes about masculinity and female sexuality, influences the way that these photographs are perceived" (Dodge, 2016, p.71). Thereby, sexual violence is normalised "because of rape culture" (Dodge, 2016, p. 73). This normalisation originates in the traditional gender norms and ideals explained in the previous chapter on Gender and War. In addition, the discussion on this topic is mainly focused on women as victims (Sida, 2019; Dodge & Spencer, 2018; Suzor et al.,2018) which indicate that gender based violence online is mainly focused on women since women are seen as the only sex to be a victim of such crimes.

In conclusion, this brief and short chapter present two topics in the literature on the relationship between gender and cyberspace. It is a very broad field and the two topics listed in this chapter are currently the more discussed topics. The following chapter will bring together the issues presented and explained in this and the previous two chapters and thereby try to answer the fourth guiding question.

6. The nexus between cyber warfare and gender

After having provided an overview of the field of hybrid warfare and cyber warfare, gender and war literature and the emerging field of gender and cyber, this chapter will attempt to bring the fields together and attend to the fourth guiding question - Drawing upon the concept of cyber warfare and its various dimensions (identified in the first

question) and the literature on gender and war as well as gender and cyber. How may cyber warfare be gendered?

This chapter consists of four sections and will follow the outline of the four main and core questions that form this thesis. The first section will look at Gunneriusson and Ottis idea of approaching cyberspace from a hybrid warfare perspective and focus on non-military targets and how it might be gendered. The second section will look into the example of propaganda, which Gunneriusson and Ottis also mentioned, and recap some of the previous research on how propaganda is gendered and explore how Stanley's conceptualisation in propaganda, more particularly Stanley's differentiation between supporting and undermining propaganda, is related to previous research on propaganda and gender, and is also gendered. Yet, and as we will see, the distinctions between the two become rather blurred when applied to gender. In addition, a few recent empirical examples will be provided in order to support the argument. The following part of the chapter will focus on what indeed seems to be new: namely the field, cyberspace, here drawing upon both on the literature on gender and war and gender and cyber. The last two sections will thus explore and discuss what it means in terms of gender that while propaganda is nothing new, the ways technology, use of cyberspace, is something new. What might the new technology mean in terms of gender? This will be followed with a final section on workplaces in the cyber security sector and gender-based violence online.

6.1 Non-military targets

In chapter 4, Gunneriusson and Ottis idea of how cyberspace can be viewed in three ways from a hybrid warfare perspective was explained. The three ways are: as supporting conventional warfare, non-military targets, and "environment" (Gunneriusson &Ottis, 2013). This section will jump straight to the second approach, because the first approach, covers cyber warfare that is combined with conventional warfare, and the focus on the fourth guiding question is cyber warfare on its own not in combination with other methods of warfare. Non-military targets are considered attacks on CII systems, and to attack CII systems successfully could "cause serious harms and physical damage" Gunneriusson &Ottis, 2013, p. 102) since societies rely heavily on these. Yet, this is currently hypothetical but still very much possible. However, physical damage is not always possible. An attack on CII can have great consequences on society, it can "cause civilian unrest or a mass evacuation in the area of operations" (Gunneriusson & Ottis,2013, p.

102). Nonetheless, the Geneva conventions state which attacks are violating international law and which are not, however, to take into account international law when planning attacks is not the first thing on the actor's priority list. Furthermore, the previous sections on general research on cyber warfare and literature on gender and war, show that cyberspace itself is gendered. The previous chapter concluded that the workforce within cyber related sectors is male dominated. Knowing that, how might an attack on non-military systems have an impact on gender roles? This section will aim to answer this by examining what are the potential targets and look at the research from gender and war field.

One possible non-military target mentioned by Gunneriusson and Ottis is a state's or cities power plants. Power plants generate electricity and an attack would lead to increased insecurity for both women and men. Research has shown that increasing insecurity mainly implicates a higher risk of being subjected to sexual violence, especially during the night (OCHR, 2012). Additionally, access to electricity is connected to access to information, thus, an attack on power plants will not only increase insecurity in society, but it will also entail that civilians will not be able to be informed on the latest news or to be able to contact anyone when in need. This consequence, no access to information, is not gendered, both women and men are affected by this in the same way as in both will not be able to access information. Another possible non-military target is water plants. In societies where there is no drinking water in the households, the chore of collecting water would clearly be affected if there is an attack on a water plant (Stockholm Environment Institute, 2019). There are no examples of how these sorts of attacks could be gendered, however looking at the gender and war literature one can make some assumptions and suggestions of possible consequences. Since it is common that women, due to social structures, are responsible for domestic chores, an attack on for example water plants could have a greater impact on women than men. In addition, research has also shown that water insecurity is much interlinked with gender, ethnicity, race, class and age (Stockholm Environment Institute, 2019).

In conclusion, there is a possibility that a cyber-attack on non-military targets such as power plant or water plant can have gendered effect. It is difficult to analyze how cyber-attack on non-military targets when there is not much research on this topic but also since the effects from a cyber-attack are contextual. With that said, there is a possibility of

effects on the gender roles in societies where women, or men, are responsible for e.g. fetching water.

6.2 Propaganda

As we have seen from the previous chapter, one major aspect included in cyber warfare is propaganda. Propaganda has, as outlined above, existed for a long time, in turn showing that the practice of hybrid warfare is not something new. Moreover, as shown in chapter 4, gender research has demonstrated how propaganda is gendered. As emphasized above, propaganda has existed for a long time with the aim to influence people's opinion(s) and gender and war literature show that the use of gendered propaganda is clearly not a new phenomenon. There are numerous examples from the world wars of gendered propaganda that had varied motives. For example, posters of women insisting more men to join the armed forces, pornographic leaflets to disturb the soldiers on the fields, and radio networks playing disturbing recordings to increase the desire to go to war. These examples can be divided into Stanley's categorization of supporting and undermining propaganda. As explained earlier, supporting propaganda aim is to "increase the realization of a political ideal" (Stanley, 2015, p.53) and by using emotion it will consequently create rational reasons to support a certain political ideal (Stanley, 2015). Translated to the field of gender and war, supporting propaganda can be understood as gendered propaganda which increases the willingness to fight by particular supporting images of the own nation and troops and the cause.

Yet, the literature on gender and war also applies to what Stanley calls undermining propaganda, which undermines a political ideal by communicate a message that is inconsistent with it. This can of course be done in various ways but learning from the literature of gender and war this sort of propaganda can be seen to encompass gendered propaganda which aims at increasing the willingness to fight by using particular gendered images of the enemy. For instance, in his book War and Gender, Goldstein concludes that "men's participation in combat depends on feminizing the enemy as symbolic domination" (Goldstein, 2006, p. 356). Hence, he shows that feminisation of the enemy might work to increase the readiness to fight by portraying the enemy as weak and non-threatening and easy to conquer and thereby associating the enemy with female traits.

A more recent example of gendered propaganda is the case for Islamic State of Iraq and the Syria (ISIS) strategy and methods to recruit women and men, yet for different purposes. Haroro J.Ingram (2015) seeks to find the purpose of ISIS's propaganda in his article and argues that their central aim is "…to shape the perceptions of its audiences- both friends and foes- and polarise their support"(Ingram, 2015, p.735). ISIS recruitment methods are multi-layered and can be explained in three levels. The first level is the central media units al-Hayat and their radio network Ajnad, the second level are wiljat provincial information offices and the third level is its broader membership and supporter base (Ingram, 2015). The central media units and radio network are focusing on a regional and local level and do so by publishing statements and news on main issues or events from ISIS's central command centre, and Ajnad play audio "nasheeds (hymns), and sura recitations" (Ingram, 2015 p.734). The wilyat information centres are more locally based and use inter alia posters and public events to propagate (Ingram, 2015). In addition, ISIS's propaganda is found on social media platforms, such as Twitter, Facebook and Youtube in order to target young and susceptible women and men (Awan, 2017).

There is an obvious majority of men who have been recruited to ISIS, and women are recruited to join the caliphate and to live up to their roles as "wives, mothers, teachers, and nurses" (van Leuven, Mazurana & Gordon, 2016, p. 103). The recruitment of women, men and young girls and boys, is founded on manipulating attributes that are considered feminine and masculine. ISIS recruiters release professionally looking videos of male fighters in combat, who poses "on captured vehicles or over the corpses of defeated enemies" (van Leuven, Mazurana & Gordon, 2016, p.107). By acknowledging the desire to feel empowered and dominant, ISIS fighters present the idea that their combatants are masculine, militarised and powerful (van Leuven, Mazurana & Gordon. 2016, p. 107). Moreover, another way ISIS is recruiting is to play on the gender norm that men are the protector. On social media platforms, ISIS recruiters release ferocious images of Sunni women and children killed in war zones requesting men to join the jihad and protect innocent and weak women and children (Europol, 2019). Another approach is questioning men why they have not joined ISIS, for example a video of a French fighter were released where he tells stories of how pregnant women managed to travel to ISIS controlled areas and he argue that men should then be able to travel to ISIS's areas as well (Europol, 2019). Another similar approach where men and women are criticised for refusing to join was when the online magazine Dabiq warned by stating "Beware of letting the affection you

have towards a loved one turn you away from aiding Allah's religion" (van Leuven, Mazurana & Gordon, 2016 p.110). This statement is based on similar idea mentioned in chapter 4 on how men were motivated to join the military but also to condemn the ones who did not participate in the war. Young men, and women, is also offered monthly allowances since these young adults are "negatively linking unemployment to religion" (van Leuven, Mazurana & Gordon, 2016 p. 108), ISIS also has a reputation of being the "highest paid opposition militia in Syria" (van Leuven, Mazurana & Gordon, 2016 p. 108). All these examples show clearly the combination of both supporting and undermining propaganda but also the difficulty to keep them separate. ISIS's methods of online recruitment take advantage of emotional and non-rational means (supporting propaganda) but also promises monthly allowances.

There are some differences when recruiting young women from Western and Eastern countries (van Leuven, Mazurana & Gordon, 2016). The strategy when recruiting from the Middle East and Central Asia is to focus on personal relationships, e.g. female prayer groups, accentuate on "traditional Muslim gender roles" such as what is written in the Women in Islamic State manifesto. When recruiting women from Western countries, the emphasis lies on the "adventure and excitement" in joining ISIS. In these cases, social media are more used, where recruiters talk about loving friendships and sisterhood (van Leuven, Mazurana & Gordon, 2016). Furthermore, in order to build a new Islamic society and to build the caliphate, which is the goal of ISIS, women are needed hence these tactics. Therefore, also older girls and women are recruited for the purpose to be wives and future mothers (van Leuven, Mazurana & Gordon, 2016). Promises of sisterhood, security, prosperity in the form of rent-free housing, food and new clothing are told by recruiters to motivate women to join them (The Carter Center,2017). Yet, women are seen as rewards for the men how decide to join (van Leuven, Mazurana & Gordon, 2016). This contradicts the promises ISIS recruiters give to women of "female liberation and empowerment" (The Carter Center, 2017, p. 5). This liberation is compared to the Western feminism which supporters argue is "an exclusionary model of emancipation for elite women at the expense of minority groups" (The Carter Center, 2017, p. 5). Moreover, these promises are based on Islamic ideals which entails that the roles of Muslim women and men are "complementary and cooperative rather than competitive", additionally they claim that "women and men are independent agents with their own spheres and are responsible for fulfilling their respective, divinely assigned duties" (The

Carter Center, 2017, p. 5). This means, as explained above, women are seen as wives and mothers, and men as combatants on the frontline, and despite their different duties they are still equal in their status as jihadis (The Carter Center,2017). This is an example of undermining propaganda as the ISIS recruiters argue for female liberation and empowerment, however, this does not mean actual liberation. Moreover, according to jihad when women stay at home and commit to the traditional roles, they are actually motivating their husband and "instill in her children the love of jihad and martyrdom"(Europol, 2019, p.3) These examples of undermining propaganda have been efficient and sympathised by many women who are marginalised by "western political and economic hegemony"(The Carter Center, 2017, p. 5).

Furthermore, it does not come as surprise that propaganda is gendered. The current examples of ISIS propaganda recruitment of women and men show how the use of cyberspace facilitate gendered propaganda and how cyberspace had not only made it easier to expand reach their audience but also more efficient and easier to send out target propaganda which are based on gender norms and ideals.

6.3 Male domain

As concluded in previous chapter, the general literature on gender and cyber is not specifically focusing on how the use of the warfare affect women and men differently, but instead on the gender gap within the industry, specifically the industry of cybersecurity. Information and communication systems, cyber warfare, cybersecurity etc. are perceived as masculine, as it is mainly men working with these subjects. Thereby, the lack of women in this industry is much due to the hegemonic masculinity. Masculinity, and femininity for that matter, changes with time yet this industry has continued to be a male dominated. In short, the cyber sphere is similar to the military in that it is dominated by men. What then might the increasing importance on cyber in warfare mean in terms of gender and war? One possibility is clearly that the increasing importance on cyber in warfare risk strengthening the military as a largely masculine domain. Yet, learning from the literature on gender and war and military institutions, another scenario is possible, and which might mean that the military actually open up for women to work with cyber warfare (compared to cyber in the civilian sphere).

As mentioned in chapter 5, to recruit more women as well to ensure there are chances of promotion has been the focal point, and the literature on feminisation of the army discussed in chapter 4, imply that cyber could – like other non-combatant roles- be particularly suitable to women. Non-combatant roles are considered more suitable to women based on assumptions on women's femininity (Baaz & Stern, 2011). Assumptions originated from feminized traits such as being beautiful souls in need of protection, patient and caring. These traits are considered acceptable with the believed work tasks as a peacekeeper, or within the industry of cyber security. This is a common mindset when recruiting women to become drone pilots. The existence of a female drone pilot is more "acceptable" since their work tasks are considered fairly feminine. According to Lorraine Bayard de Volo(2016), "drones unsettle militarized masculinity" (Bayard de Volo, 2016 p.57). Courage, honour and physical strength are three traits that are considered masculine and necessary to exist if one is in the armed forces, however, these traits are not necessary for a drone pilot to express therefore women are considered suitable to work as drone pilots (de Volo, 2016; Masters, 2018).

Moreover, it was and probably still is common to argue that the physical and emotional differences are why men are more suitable to join the military, however, as arguments regarding physical strength dissolved, the arguments on women being weak emotionally continue to be used (de Groot, 2001). Thereby one could argue that cyberspace, as a male domain would strengthen the military and specifically cyber warfare masculine traits. Nevertheless, since there is an increase of women in the ranks and it is a workplace where it is not necessary to show masculine attributes such as psychical strength or actually to be present in the war zones, cyber warfare can be constructed as suitable for women.

With that said, cyberspace and cyber warfare are associated with masculinity and masculine traits and it has thus become difficult for women to become part of that sector. Gender and war literature have explained that masculine and feminine traits affect the division of labour but also that there are parts of the military's work that is feminised, the peacekeeping missions. The reasons for feminising peacekeeping mission are parallel to how some argue cyber related workplaces should be femininized. With the public debate on the issue of lack of women as well as on the gender norms this domain is built on, this field might move towards a more gender neutral or even feminised domain for the same reasons peacekeeping missions and drone warfare are feminised.

6.4 Gender-based violence online

As Charlotte Isaksson stated in her chapter in the Handbook on Cybersecurity (Rehrl, 2018) the expansion of cyberspace has had both positive and negative consequences from a and individual level. Gender-based violence is a weapon of war. It is a common tactic of state and non-state actors, despite it being a violation of international law. It is a method to terrorize a population, as well as to dominate a territory and a way to humiliate the victims of the violence as well as their opponents. In the previous chapter and the previous section on gendered propaganda, examples of how gender-based violence is used in propaganda have been presented. It can be both threats from opponents that gender-based violence will be used, a state warning its citizens through different platforms "that the bad guys do bad things to them" or a way to provoke opponents' soldiers through for example playing recordings of gangrapes.

With that said, the chapter on gender and cyber showed that cyberspace facilitates gender-based violence. This raise the question what does this mean in regard to the focus of this thesis, cyber warfare? It is not an easy question since this is a rather new topic. The phenomena of gender-based violence online has received much attention from the UN and the EU yet the focus on warfare or during wartimes is not much discussed. A suggestion is that gender-based violence can be used just as it has done for thousands of years, for propaganda purposes. The difference is that it occurs online. Gender-based violence can be used to provoke opponents or to provoke its own population in order to increase support for engaging in war or for patriotism. Additionally, it will continue to be threat for the ones who do not support an operation or supports the enemies. Whether it is online or offline gender-based violence the aim of the method will continue to be the same. Gender-based violence online or offline will still be based on feminising the enemy, the main difference is that when it is on cyberspace the outreach and information about the conduct will be known quicker, and in regards to warfare it will still be used to threaten or provoke an enemy or its own citizens.

7. Concluding Discussion

At first this thesis was supposed to analyse how international organizations' policies and strategies include a gender perspective, yet early on it became clear that it would be rather difficult since there is a research gap on the gendered aspects of cyber warfare. From the

main and complex research question - What can the literature within the "Gender and War" and "Gender and Cyber" fields teach us about how cyber warfare may be gendered? emerged four guiding questions that formed the structure of this thesis. Moreover, it is important to repeat that this thesis is a theoretical attempt to fill the research gap on the gendered aspects of cyber warfare. The thesis covered two main fields of research and the general literature on cyber warfare. The application of these two main fields of research on cyber warfare is not the easiest due to the research gap. The previous chapters presented varied ways on how different fields in warfare is gendered, and to summarize, the sixth chapter brought the main ideas from the previous chapters and followed the approach of Gunneriusson and Ottis illustration on how one can categorize cyberspace in military operations, from a hybrid warfare perspective, and added Stanley's complicated approach of defining propaganda. This last chapter will summarize and discuss the outcome of the previous chapter.

The first example of how cyberspace can be approached in regard to military operations is non-military targets such as power plants and water plants. Some of the main consequences from attacking power plants are increased insecurity, and the consequences from such cyber-attack affect both women and men. Based on traditional gender norms one could argue that in these situations the traditional gender norms become more visible since women are portrayed as weak and vulnerable but also because their bodies are constantly sexualized thus increasing the risk for e.g. sexual violence. But on the other hand, this could as much be the case for men. A cyber-attack on a water plant can be linked to the division of labour and how the division is based on traditional gender norms. Previous chapter concludes that there are some possible gendered affects, but it all comes down to context. Thus, non-military targets might have gendered affects, but it is not always obvious since the context determines how it will affect women and men and their roles.

The second example, propaganda, is gendered whether it is online or offline. The more up-to-date examples of how propaganda is used online indicate that both state and non-state actors take advantage of spreading propaganda online. Stanley's conceptualisation seemed to not clarify the complexity of the topic but rather the opposite. Nonetheless, it is clear that cyber warfare in regard to propaganda is gendered even depending on the means and targets. This concludes that cyberspace's role is making propaganda a more

efficient and advantageous for the perpetrator. Although, propaganda online can take on different forms, propaganda use traditional gender norms and ideals to get more support.

The third example, but also the fourth example, are more influenced from the general literature on gender and cyberspace. The discussion on cyber warfare being a male domain is based on the perception and association of cyber related workplace with masculine traits. There are some clear similarities to the phenomena of feminisation of peacekeeping and drone warfare, and thereby indicate that there are gendered effects. This is perhaps too obvious since the cyber warfare is a male domain at start and based on gender norms that form certain masculine traits. These traits are clearly affecting women and their roles in war, in regard to both the work field as well as to who is conducting cyber warfare. Simultaneously, these traits explain the lack of knowledge on possible effects since the focus is mainly on the man.

The last and fourth example that is brought up is gender-based violence, and it can be concluded with the same logic as was done with online propaganda. The reasoning and method for gender-based violence are the same as it would be online or offline and from what was shown in the overview of the general literature on gender and war as well as gender and cyber is that it is clearly gendered. The linkage to warfare is not as clear, but one can conclude that gender-based violence online can be used for the same purpose as gender-based violence in propaganda has been using it for centuries.

The two main fields of literature that is concentrated on in this thesis clarified that some aspects in cyber warfare are clearly gendered- propaganda, gender-based violence online, and the working sector. Furthermore, these three examples of cyber warfare are not explicit examples of cyber warfare. Gender and war literature showed that propaganda has existed before the existence of cyberspace, it is a common method of warfare just as gender-based violence is unfortunately a common method of warfare. The cyber dimension offers another field to conduct warfare, but the purpose is still the same in regard to propaganda and gender-based violence. This could perhaps be one explanation to why a gendered aspect of cyber warfare is not a well discussed topic. One example that is perhaps not as clear is cyber-attacks on non-military targets. It is difficult to analyse the gendered aspects since it all comes down to geographical location of the target, what the target is, and the relation society has to the target. Moreover, as mentioned in the

introductory chapter, the possible gendered effects are more or less based on context. If another categorisation of cyber warfare had been used there would be have been other outcomes. This also clarifies the ongoing debate on the existence of hybridity and whether hybrid warfare is a new concept since much of the methods explained are not new. What is new is the domain, cyberspace. With that said, one cannot disregard the gendered effects and that the consequences of cyber warfare might have greater effect than other methods of warfare.

In conclusion, this first theoretical attempt to fill the research gap signals that this thesis is discussing a topic that needs more recognition since even if propaganda, gender-based violence online, targeting non-military targets and the workplace show that the cyber dimension gives the perpetrators the possibility to intensify the consequences of an attack, there are still questions regarding the gendered aspects of cyber warfare: Is it possible for cyber warfare to be gender neutral? How do the gendered examples of cyber warfare appear when it is used in combination with other warfare methods? What influence do the examples of gendered cyber-attacks have on hybrid warfare? In other words, it is necessary to give more attention to the nexus between cyber warfare and gender.

References

Arquilla, J & Ronfeldt, D. (1993). Cyberwar is coming!. *Comparative Strategy, Vol. 12* (2), p. 141-165. Retrieved from: <https://www.rand.org/pubs/reprints/RP223.html>.

Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. *Social Science and Public Policy Vol. 54*, p. 138-149. Doi: 10.1007/s12115-017-0114-0.

Bachmann, S.D. & Gunneriusson, H. (2015). Hybrid Wars: Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security. *Scientia Militaria, South African Journal of Military Studies*, [e-journal] 43(1) p.77-98. Doi: 10.5787/43-1-1110.

Bayard de Volo, L. (2016). Unmanned? Gender recalibrations and the rise of drone warfare? *Politics & Gender Vol. 12* (1), p. 50-77. Doi: 10.1017/S1743923X15000252.

Baaz, M.E & Stern, M. (2011). Whores, Men, and Other Misfits: undoing 'Feminization in the armed forces in the DRC. *African Affairs, Vol. 110* (441), p. 563-585. Retrieved from: <https://www.jstor.org/stable/41240236>.

Betz, D. (2019). The Idea of Hybridity. In. Fridman, O., Kabernik, V & Pearce, J.C.,2019. *Hybrid conflicts and information warfare: new labels, old politics* (p. 9-25). Boulder; London: Lynne Rienner Publishers.

Bjarnegård, E., Melander, E., Bardall, G., Brounéus, K., Forsberg, E., Johansson, K., Muvumba Sellström, A., Olsson, L. (2015). Gender, peace and armed conflict. In. Davis, I (ed.), *SIPRI Yearbook 2015: Armaments, Disarmament and International Security* (p. 101-109). Oxford: Oxford University Press.

The Carter Center. (2017). The Women in Daesh: Deconstructing Complex Gender Dynamics in Daesh Recruitment Propaganda.

Carpenter, R. C. (2006). *Innocent women and children: gender, norms and the protection of civilians.* Ashgate Publishing Limited.

Carpenter, R. C. (2006). Recognising Gender- based Violence Against Civilian Men and Boys in Conflict Situations. *SAGE publications Vol. 37* (1), p. 83-103. Doi: 10.1177/0967010606064139.

Caliskan, M & Cramers P.A. (2018). What Do You Mean by "Hybrid Warfare"? A Content Analysis on the Media Coverage of Hybrid Warfare Concept. *Horizon Insights Vol. 4* (October-December), p. 23-35. Doi: 10.31175/hi.2018.04.

Cornish, P., Livingstone, D., Clemente, D., Yorke, C. (2010). *On Cyber Warfare (A Chatham House report).* Chatham House.

Chen, J & Dinerman, A. (2016). On Cyber Dominance in Modern Warfare. *European Conference on Cyber Warfare and Security.* Retrieved from: <https://search.proquest.com/openview/9ed6393bce9c040007ba80f892744b2c/1?pq-origsite=gscholar&cbl=396497>.

De Groot, G. J. (2001). A few good women: Gender stereotypes, the military and peacekeeping. *International Peacekeeping, Vol.8* (2) p. 23-38. Doi: 10.1080/13533310108413893.

Denov, M & Ricard-Guay, A. (2013). Girl soldiers: towards a gendered understanding of wartime recruitment, participation, and demobilisation, *Gender & Development, Vol. 21* (3), p. 473-488. Doi: 10.1080/13552074.2013.846605.

Dodge, A. (2016). Digitizing rape culture: Online sexual violence and the power of the digital photograph. *Crime Media Culture, Vol. 12* (1), p. 65-82. Doi: 10.1177/1741659015601173.

Dodge, A & Spencer, D.C. (2018). Online Sexual Violence, Child Pornography or Something Else Entirely? Police Responses to Non-Consensual Intimate Sharing among Youth. *Social & Legal Studies, Vol. 27* (5), p. 636-657. Doi: 10.1177/0964663917724866.

Ehlstain, J.B. (1982). On Beautiful Soul, Just Warriors and Feminist Consciousness. *Women's Studies International Forum, Vol. 5,* (3/4), p. 341-348. Doi: 10.1016/0277-5395(82)90043-7.

Enloe, C.H.(2000). *Bananas, beaches and bases: making feminist sense of international politics*. Berkeley: University of California Press.

Enloe, C.H. (2000). *Manoeuvres: the international politics of militarizing women's lives*. Berkeley: University of California Press.

Enloe, C. (2004). *The Curious Feminist.* Berkeley: University of California Press.

Europol. (2019). Women in Islamic State Propaganda Roles and Incentives. Europol Specialist Reporting. Retrieved from<:https://www.europol.europa.eu/activities-services/europol-specialist-reporting/women-in-islamic-state-propaganda >.

Fridman, O. (2019). A War of Definitions: Hybridity in Russia and The West. In. Fridman, O., Kabernik, V & Pearce, J.C. *Hybrid conflicts and information warfare: new labels, old politics* (p.67-87). Boulder; London: Lynne Rienner Publishers.

Fridman, O., Kabernik, V & Pearce, J.C.(2019). *Hybrid conflicts and information warfare: new labels, old politics.* Boulder; London: Lynne Rienner Publishers.

Gentry, C.E & Sjoberg, L., (2015). *Beyond mothers, monsters, whores: thinking about women's violence in global politics.* London: Zed Books.

Giergerich, B. (2016). Hybrid Warfare and the Changing Character of Conflict. *Connections: The Quarterly Journal, Vol.15* (2). Available at: <https://www.jstor.org/stable/10.2307/26326440> [Accessed 3 October 2019].

Goldstein, J.S. (2006). *War and gender: how gender shapes the war system and vice versa.* (2nd ed., 3rd printing), Cambridge: Cambridge University Press.

Gunneriusson, H & Ottis, R. (2013). Cyberspace from the Hybrid Threat Perspective. *Journal of Information Warfare, Vol. 12* (3), p. 67-77. Retrieved from: <https://www.jstor.org/stable/26486843>.

Habgood-Coote, J. (2019). Stop talking about fake news!. *Inquiry, Vol. 62* (9-10), p. 1033-1065. Doi:10.1080/0020174X.2018.1508363.

Hasler, J.L. (2007). Defining War: New doctrinal definitions of irregular, conventional and unconventional warfare. *Special Warfare.*

Heickerö, R. (2010). Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. FOI, Swedish Defence Research Agency.

Hoffman, F.G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.

Hoffman, F.G. (2009). Hybrid Warfare and Challenges. *JFQ, Vol. 52* (1), p. 34-39. Retrieved from: <https://smallwarsjournal.com/documents/jfqhoffman.pdf>.

Hoffman, F. G. (2018). Examining Complex Forms of Conflict. Gray Zone and Hybrid Challenges. *PRISM - The Journal of Complex Operations Vol. 7* (4) p. 31-47. Retrieved from: <https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/>.

Höglund, A. T. (2010). *Gender and the War on Terrorism - the justification of war in a post 9/11 perspective.* Uppsala: University Printers.

Ingram, H.J. (2015). The strategic logic of Islamic State information operations. *Australian Journal of International Affairs Vol. 69* (6), p. 729-752. Doi: 10.1080/10357718.2015.1059799.

Johnson, R. (2017). Hybrid War and Its Countermeasures: A Critique on the Literature. *Small Wars & Insurgencies, Vol. 29* (1), p. 141.163. Doi: 10.1080/09592318.2018.1404770.

Jones, A. and Kovacich, G.L .(2016). *Global Information warfare: the new digital battlefield*. (2nd ed.), Boca Raton: CRC Press/Taylor & Francis Group.

Jowett, G & O' Donnell, J. (2006). *Propaganda and Persuasion.* Thousand Oaks: Sage Publications.

Karim, S.M & Henry, M. (2018). Gender and Peacekeeping. In. Ní Aoláin, F., Cahn, N., Francesca Haynes, D., Valji, N (eds.), *The Oxford Handbook on Gender and Conflict.* Doi: 10.1093/oxfordhb/9780199300983.013.3.1.

Kramarae, C & Spender, D. (2000). Routledge International Encyclopedia of Women-Global Women's Issues and Knowledge. Routledge.

Libicki, M.C. (1995). *What is Information Warfare?.* Washington: National Defense University, Institute for National Strategic Studies.

Macdonald, K.S. (2007). *Contemporary Security Studies Series: Propaganda and Information warfare in the twenty-first century: altered images and deception operations*. London: Routledge.

Masters, C. (2018). Gender, Violence, and Technology. In. Gentry, C.E., Shepherd, L.J and Sjoberg, L. (eds.), *Routledge Handbook of Gender and Security.* London: Routledge.

Melzer, N. (2011). Cyberwarfare and International Law. *Ideas for Peace and Security.* Retrieved from: <https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>.

OCHR. (2012). *Violence and Insecurity: Protecting human rights in situation of violence and insecurity.*

Peacock, D & Irons, A. (2017). Gender Inequalities in Cybersecurity: Exploring the Gender Gap in Opportunities and Progression. *International Journal of Gender, Science*

and Technology, Vol. 9 (1), p. 25-44. <http://genderandset.open.ac.uk/index.php/genderandset/article/view/449>.

Rehrl, J. (2018). *Handbook on Cybersecurity - The Common Security and Defence Policy of the European Union.* Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria. Retrieved from: <https://op.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1>.

Schnaufer. T. A. (2017). Redefining Hybrid Warfare: Russia's Non-linear War against the West. *Journal of Strategic Security, Vol. 10* (1), p. 17-31. Doi:10.5038/1944-0472.10.1.1538.

Sida. (2019). (Brief) Gender-Based Violence Online.

Sjoberg, L & Peet, J. (2011). A(nother) Dark Side of the Protection Racket- Targeting Women in Wars. *International Feminist Journal of Politics, Vol. 13* (2), p. 163-182. Doi: 10.1080/14616742.2011.560751.

Sjoberg, L.(2014). *Gender, War and Conflict.* Cambridge: Polity Press.

Stanley, J. (2015). *How Propaganda Works.* Princeton University Press.

Stockholm Environment Institute. (2019). Exploring gender dimensions of water insecurity and governance in the Lower Mekong Region. Retrieved from: <https://www.sei.org/publications/exploring-gender-dimensions-of-water-insecurity-and-governance-in-the-lower-mekong-region/>.

Suzor, N., Dragiewicz, M., Harris, B., Gillett, R., Burgess, J., Van Geelen, T. (2018). Human Rights by Design: The responsibilities of Social Media Platforms to Address Gender-Based Violence Online. *Policy & Internet, Vol. 11* (1), p. 84- 103. Doi: 10.1002/poi3.185.

Yesil, B. (2004). ‘Who Said this is a Man’s War?’: propaganda, advertising discourse and the representation of war worker women during the Second World War. *Media History, Vol. 10* (2), p.103-117. Doi: 10.1080/1368880042000254838.

Van Leuven,D., Mazurana, D., Gordon, R. (2016) Analysing the Recruitment and Use of Foreign Men and Women in ISIL through a Gender Perspective. In. de Guttry, A., Capone, F., Paulussen, C (eds.), *Foreign Fighters under International Law and Beyond* (p. 97-120). T.M.C. ASSER PRESS.

Welland, J., (2018). Gender and War. In Gentry, C.E., Shepherd, L.J and Sjoberg,L (eds.), *Routledge Handbook of Gender and Security.* London: Routledge.

Wither, J.K., (2016). Making Sense of Hybrid Warfare. *Connections: The Quarterly Journal,* [e-journal] 15(2) p. 73-87. Doi: http://dx.doi.org/10.11610/Connections.15.2.06.

Winterfeld, S. and Andress,J. (2013). *The Basics of Cyber Warfare: understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Amsterdam; Boston: Syngress.