Swedish Defence University

Why is human trafficking excluded from the EU's cybersecurity?
An explorative study about cybersecurity and human trafficking in the European Union

Linda Nieminen

Master's thesis, 30 ECTS (hp)
Political Science with a focus on Crisis Management and Security
Master's Programme in Politics and War
Autumn 2020
Supervisor: Magnus Ekengren
Word count: 12 589

Abstract

Combatting human trafficking is one of the top priorities in the European Union and Europol. Nonetheless, Europe is one of worlds' leading regions for most trafficked human beings. Human trafficking is often connected to organised crime such as drug trafficking, cybercrime and child pornography and occurs across borders. 21st century's digital age has broadly shifted human trafficking from the real-life to the cyberspace. However, human trafficking is not mentioned in any EU cybersecurity policies.

This thesis aims to explore, using a feminist security approach, why human trafficking is overlooked in the European Union cybersecurity. By conducting an interpretive content analysis and using the method of deconstruction, I investigated the silences of human trafficking and gender. Leaning on feminist theories of securitisation, hegemonic masculinity and poststructural feminism, three significant assumptions were identified. The first assumption was that human trafficking is overlooked in the EU cybersecurity because of the non-human referent object of security. The second was that it is overlooked because of hegemonic masculinity. And lastly, because the issue is seen as private and therefore do not belong to cybersecurity. By analysing EU cybersecurity policies, I identified that the EU cybersecurity is dominated by norms of hegemonic masculinity and gendered social hierarchies. In the EU cybersecurity, threats related to non-human objects are constructed and gain hegemony over human rights and social policies. This study has raised important questions about the nature of cybersecurity in the EU, and greater efforts are needed to ensure women's security in the cyberspace. These results suggest that if the EU aims to combat human trafficking wholehearted, it needs to start with acknowledging human trafficking as a threat in the cyberspace.

Key words: Cybersecurity, European Union, human trafficking, feminist theory, securitisation, hegemonic masculinity, poststructural feminism

Table of content

1. Introduction

> "*It should be possible to write the body into a discipline that tracks power relations and practices which impact so directly and often so devastatingly on actual bodies*" (Pettman, 1997, p. 105).

What if someone told you that men build the world we live in for men, and that is why women are more insecure in this world, as it is not formed to fit them. That women are in more risk of injury in car accidents because car seat belts are designed for men that often sit further back when driving. That the average size of mobile phones doesn't fit women's hands because it is designed after men's bigger hands. That speech recognition software is usually better to recognize a man's voice because it is trained on recordings of male voices (The Guardian, 2019). And that a woman is 20 times[1] more likely to be a victim of sexual exploitation than a man (European Institute for Gender Equality, 2018). A long time ago, tailors worked with the knowledge that women and men have different shapes. Taylors sewed suits to fit perfectly the distinct shape of women and men. Somehow, this knowledge about different forms has failed to pass through many other areas of design.

Some people say that slavery is long gone in history. That it doesn't happen anymore, it just magically vanished into the air. Unfortunately, these assumptions are wrong. After all, slavery has only changed its name and is a more significant issue than ever before. Human trafficking is modern-day slavery. Human trafficking for sexual exploitation is a huge problem and security issue for women in the European region (Hughes, 2014). The Anti-Trafficking Directive (Article 2) in the European Union defines trafficking in human beings as:

> "*the recruitment, transportation, transfer, harbouring or reception of persons, including the exchange or transfer of control over those persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of*

[1] European Institute for Gender Equality, 2018. "Regarding trafficking for the purposes of sexual exploitation, 96 % of detected victims in the world are female" p. 13

payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation" (Directive 2011/36/EU. Article 2:1).

Globalization and new information technologies have partly shifted social activity to cyberspace. Over the past 20 years, the internet has had an extensive impact on our society. Consequently, many parts of our daily life now depend on the internet working uninterruptedly. Likewise, our "real life" has transferred partly to cyberspace, so has criminal activity (European Commission, 2013; Hughes, 2014; Latonero, 2012). Criminals capacity to traffick human beings has tremendously expanded from the traditional way of recruiting and selling people in the real-life to the global cyberspace. Organized crime groups involved in human trafficking have now broadened ability to traffick human beings for diverse types of exploitation (Thakor & Boyd, 2013; Hughes, 2014; Latonero, 2012; Europol, 2020). Technology allows traffickers to communicate instantly with potential victims and indeed, for large audiences of "buyers" across geographic boundaries and long distances. Visibility, transaction, coordination and organization are impacted by digital and networked technologies, consequently impacting the whole trafficking process. Grooming, recruitment, domination over victims, advertising, moving and economical transactions are now frequently affected by the broad opportunities 21st century's digital age has brought (Latonero, 2012, p. 10). Nevertheless, the perpetrators' capacity to use the internet for trafficking, the fundamental crime remains the same. A trafficker bluffs, intimidates or exploits the vulnerability of a potential victim in the purpose of exploitation. (Hughes, 2014, p. 1)

Human trafficking is a severe violation of fundamental human rights. Human rights are in the heart of the European Union. Indeed, the European Union is based on a commitment to value fundamental human rights for EU citizens and promote these values worldwide (European Union, 2020). Human rights are of utmost importance in the European Union, and the Council of Europe and EU policy includes strongly combatting against human trafficking. However, it is indeed worrying how the region of Europe can still be the worlds leading region for human trafficking for sexual exploitation at present (Hughes, 2014; Clark, 2003; Council of Europe, 2002). Besides, trafficking for the purpose of sexual exploitation is the most common form of trafficking in human beings in the European Union (European Institute for Gender Equality, 2018, p. 13). The EU's anti-trafficking strategy has identified gender inequalities being amongst the root causes of trafficking. Moreover, the EU has recognized that trafficking in human beings is a gender-specific phenomenon in its policy and legal framework. Therefore, it has called on

the Member States to adopt gender-specific measures against human trafficking (European Institute for gender equality, 2018).

However, if trafficking is a gendered crime and the crime scene in the 21st century's digital age is broadly in cyberspace, how are these gender-specific measures not adopted in the EU's cybersecurity strategy as it is the base for securing the cyberspace? Silence on gender is a significant area of interest for feminist research within international relations, and feminist analyses of human trafficking have challenged the traditional security framework. Jennifer Lobasz (2009) has shown that gender constitutes the whole concept of trafficking, and that policy focus depends on what is seen as a referent object of security (Lobasz, 2009, p.32). Andrew Liaropoulos (2015) has argued that present cybersecurity policies do not safeguard users in cyberspace as focus often lies on protecting national security (Liaropoulous, 2015, p. 18). According to Julia Slupska, the emerging dynamics of excluding women in international relations seems to repeat in the field of cybersecurity (Slupska, 2019, p. 87). Furthermore, a group of specialists in the Council of Europe researched ”the impact of new information technologies on trafficking in human beings for the purpose of sexual exploitation” and found out that the sex industry and the internet are closely intertwined. However, research on the link between these two is unprecedented (Council of Europe, 2002). Why is the trafficking of human beings not issued at all in the strategy for the European Union cybersecurity? Is it because the EU does not see human trafficking as a crime related to the cyberspace? Or because it is a gender-based crime and therefore not recognized in institutions with hegemonic masculinity? Or is the issue of human trafficking too private to be included in the field of cybersecurity? Gender inequality is not just a problem with social injustice; it is a problem for our security. With my thesis, I aim to contribute to cybersecurity scholarship that is lacking feminist research. Besides, using a feminist security approach, this thesis is at the heart of our understanding of why human trafficking is overlooked in the European Union cybersecurity. It is time for the European Union to consider the knowledge of different shapes of women and men and bring them into policy areas where they matter.

2. Aim of the research

Combatting human trafficking is one of the top priorities in the European Union and Europol. Nonetheless, Europe is one of worlds' leading regions for most trafficked human beings and the number of registered victims in the period 2015-2016 in the European Union was 20 532 human beings (European Commission, 2018). Human trafficking is often connected to organized crime such as drug trafficking, cybercrime and child pornography and occurs across borders (European Commission, 2020). Human trafficking has broadly shifted from the real-life to the cyberspace. However, it is not mentioned in any EU cybersecurity policies. Therefore, this research aims to explain, using a feminist security approach, why human trafficking is overlooked in the European Union cybersecurity.

This study will be an explorative study, and therefore, instead of using research questions, I will base my analysis on three different hypotheses based on three theories. These hypotheses can also be seen as "lenses" or "perspectives". This study will qualitatively test the following assumptions:

- Hypothesis 1: Human trafficking is overlooked in the European Union cybersecurity because of the non-human referent object of security.

- Hypothesis 2: Human trafficking is overlooked in the European Union cybersecurity because of hegemonic masculinity.

- Hypothesis 3: Human trafficking is overlooked in the European Union because the issue is seen as a private matter and, therefore, do not belong to cybersecurity.

3. Previous research

3.1 Human trafficking and technology

Feminist analyses of human trafficking have challenged the traditional security framework. Jennifer Lobasz (2009) shows in her study that gender constitutes the whole concept of trafficking human beings. Changing the course of the security of the state to the security of trafficked persons recognises that both traffickers and the state by and of itself pose security threats. Lobasz offers an explanatory approach for analysing human trafficking and shows that policy focus depends on the referent object of security (Lobasz, 2009, p. 32).
Michele Anne Clark (2003) identifies that environments that are supposed to be safe for women and children such as their families, communities and public places of business and commerce are actually increased risk-zones for them (Clark, 2003, p. 248). Age and gender increase vulnerability, but economic aspects, organised crime, civil war and political unrest make vulnerable individuals even more vulnerable to trafficking. Actors that benefit from financial rewards from trafficking are many. According to Clark, these actors are spread across international borders from recruiters to police officers, government and in some regions, even the families of those individuals exploited (Clark, 2003, p. 249). She also highlights that economic, informational and technological growth has made the sex industry more globalised and more expansive and more profitable (Clark, 2003, p. 252).

Mark Latonero (2012) researched the phenomenon of using technology in the trafficking of human beings to identify the threats and opportunities it brings in the digital age. An investigation based in the US proposes that the increase in mobile devices and networks has made them central to minors' sex trafficking in the US. According to Latonero, electronically enabled trafficking is more adaptive and diffuse than thought initially because it is spread so broadly on the internet (Latonero, 2012). Greiman and Bain (2013) present a working definition of the concept "cyber trafficking" they developed to describe the reach of trafficking online. They conclude:

> "*'Cybertrafficking' is the 'transport of persons,' by means of a computer system, Internet service, mobile device, local bulletin board service, or any device capable of electronic data storage or transmission to coerce, deceive, or consent for the purpose of 'exploitation'. Exploitation shall include, at a minimum, the exploitation of the*

> *prostitution of others or other forms of sexual exploitation, forced labor or services, slavery or practices similar to slavery and servitude. 'Transport in persons' shall mean the recruitment, advertisement, enticement, transportation, sale, purchase, transfer, harbouring or receipt of persons, for the purpose of exploitation with or without the consent of the victim.*"
> (Greiman & Bain 2013, p. 43)

Greiman and Bain show in their study that cyber trafficking can be divided into three categories. According to them, the first category includes "*use of the internet, text messaging, digital cameras, and mobile devices/smartphones to offer, advertise, and sell sex services, some of which are provided by trafficked victims*". They argue that the substantial majority of trafficking for sexual exploitation in the US is advertised and organised on the internet. However, they note that there is no empirical data available that could support this argument, and therefore their argument is only supported by anecdotal evidence (Greiman & Bain 2013, p. 43-44). The second category includes: "*identifying, locating, enticing, and recruiting new victims into trafficking and them helping to control the victims once they have been trafficked*". This activity can happen through different social networking sites or other direct communication tools. The third category includes: "*both the advertising and the delivery of coerced sex services over the internet*". These services can be forced sex acts performed to customers via web cameras or different chat rooms. This type of activity is called "cybersex" (Greiman & Bain 2013, p. 44). In 2003 a group of specialists in the Council of Europe conducted a research on "the impact of new information technologies on trafficking in human beings for the purpose of sexual exploitation" and found out that the sex industry and the internet industry are closely intertwined. However, research of the link between these two is still widely unprecedented (European Council, 2002, p. 93).

3.2 Cybersecurity and securitization

Cybersecurity as a policy topic is highly contested regarding how it is secured, by whom and why (Deibert, 2018; Slupska, 2019). Multiple different stakeholders are involved when securing cyberspace such as businesses, government agencies and civil society. Threat environment has also shifted from concerning threats posed by other states to threats that no longer have no boundaries, across all of society coming from outside and inside of states (Deibert, 2018, p. 2). Ronald Deibert (2018) explains that it has consequences that the United

States government has defined cyberspace as “a domain within which to project power, and to fight and win wars” resulting in system-wide effects both ideationally and materially since the US is the world’s largest military (Deibert, 2018, p. 3). In a study conducted by Myriam Dunn Cavelty (2012), she shows that the ways threats and risks are framed come with social and political effect, and therefore, framing is not only a matter of choice. She means that cyberspace has been militarised as cyber threats are seen as the prime focus in the debate of present national security, and therefore, cybersecurity is socially constructed. Dunn Cavelty argues that militarisation of cyberspace leads to a zero-sum game between the states, in which one state’s gain is another state’s loss. This atmosphere of insecurity and tension between states is based on misperceptions of the risks and overlooks economic and business solutions as the focus lies on national security measures (Dunn Cavelty, 2012, p. 142).

Lucas Kello (2013) argues that because cybersecurity analysis has mostly capitulated to the technologists, it has consequences for the public perceptions of cyber issues. Cyber threats are seen as destructive lines of codes, and therefore the human aspect is overlooked, such as human agents who utilise those codes and motives for that. Also, security is seen as the safety of computer networks. Therefore, a critical activity beyond cyberspace is left without attention (Kello, 2013, p. 16). Deibert (2018) describes cyberspace as a continuously evolving ecosystem contingent on local politics, geography, culture and technology. He argues that it would be ideal if politics were left out of cybersecurity hence impossible in real life. It doesn’t matter if solutions to cybersecurity issues are techno-functional; it is always a competition between different worldviews, ideologies and strategic interest (Deibert, 2018, p. 3). Deibert refers to Dunn Cavelty’s (2012) explanation of socially constructed cybersecurity and extends it to the international realm. As he does so, he means that “competing threat perceptions of cybersecurity manifest themselves”. The predominant main of cybersecurity in liberal, democratic countries is to protect information networks and different databases while ensuring free information flow to preserve the global economy. However, for the historical and institutional reasons, military and intelligence agencies hold dominant cybersecurity roles that are not tasked to protect free and open networks, but to protect national security. Therefore, there is a conflict between these competing threat perceptions - referent objects - of security (Deibert, 2018, p. 5). The issue underlying the competing paradigms of cybersecurity is, according to Deibert: “should the interest of national security trump user security? If so, when?” (Deibert, 2018, p. 7).

Turning the gaze towards the underlying issue of cybersecurity, Andrew Liaropoulos (2015) highlights the need to break the link between cybersecurity and the traditional national security concept. Using a human-centric approach in his study, Liaropoulos addresses that cybersecurity needs to include digital human rights violations, the privacy of data and internet freedom into the sphere of protecting national security (Liaropoulos, 2015, p. 15). Referring to Dunn Cavelty (2012) work on militarised discourses on cybersecurity and Jervis (1978) work on the classic security dilemma, Liaropoulos proposes that only seeing cybersecurity through the lenses of traditional national security leads to militarisation of the cybersecurity and therefore, leads to a cybersecurity dilemma (Liaropoulos, 2015, p. 17). Liaropoulos concludes that present cybersecurity policies do not safeguard users in cyberspace (Liaropoulos, 2015, p. 18).

Barry Buzan (1997) argues for a widened definition of security. According to Buzan, security should not be seen only as a traditionalist thinking of military threats but as a more general definition (Buzan, 1997, p. 9). The Copenhagen school framework is known for its widened security agenda. The view of security studies in the Copenhagen school is radical by examining threats to referent objects securitised. The process of analysing the logic of security itself makes it possible to distinguish the dispute between the traditionalist view of security and the widened view of security. Buzan means that it can be found from the traditional military-political understanding of security, what makes something a threat to international security. According to Buzan, security is always about survival. For threats and vulnerabilities to count as security issues, they need to differentiate from the political normative. In other words, they need to be seen as threats to a referent object by a securitising actor (Buzan, 1997, p. 13). The referent object is the one being secured from an acknowledged threat. Securitisation produces different kinds of discourses which gain hegemony over human rights and social policies (Ericson, 2018, p. 96).

The concepts of securitisation and de-securitisation have affected security studies since the 1990s. Seeing security as a process where threats are constructed or de-constructed is comprehended from the view of security as a state of being (Nunes, 2015). Sabine Hirschauer (2020) carried out a study of sexual violence at the time of post-World War II. She shows insights into silence production, using the concept of de-securitisation. According to her, sexual violence during the post-World War II was de-securitised as active silence (Hirschauer, 2020, p. 219). The mass rapes convicted by US, British, French and Soviet allied troops were bypassed by the process of politicisation which facilitated Germany's state identity as a "new, good" Germany (Hirschauer, 2020, p. 220).

3.3 Silencing gender

In the field of international security, silence toward gender becomes exaggerated (Wadley, 2009, p. 39). Klara Ellerby (2013) is one of the feminist researchers that has studied complexities of women's inclusion in peace processes. Ellerby demonstrates that excluding studies examining how women are not included in different kinds of peace processes affects real-life practices. Therefore, studying women's exclusion in security processes involves understanding what security is, who are deemed as relevant and legitimate actors and who gets access to resources (Ellerby, 2013, p. 437).

Institutions of hegemonic masculinity have historically excluded women's bodies, and masculinity norms have dominated their practices (Kronsell, 2005, p. 281). Masculinity theorists argue that government institutions have traditionally been male-dominated and that these institutions that make up the state also continues to be so (Blanchard, 2014, p. 71). Annica Kronsell (2005) states that institutions relevant to international relations such as defence, military and security-related institutions are marked by hegemonic masculinity. These norms shaped by exclusively including men, have influenced both policies, agendas and politics of these institutions (Kronsell, 2005, p. 281). According to her, the norms of masculinity don't need to be thematised because they remain reproduced by these institutions' routines (Kronsell, 2005, p. 283). She argues that if institutions with hegemonic masculinity open up to the "other" and depart from strict gender segregation, institutional change and development could happen simultaneously changing gender relations (Kronsell, 2006, p. 109).

Furthermore, Kronsell (2016) highlights in her study that the European Union's security and defence policy (CSDP) is male-dominated. However, the gendered male domination is invisible through normalisation in the institution of the EU. She argues that the CSDP embraces diverse types of military masculinities. The relation between these different types of masculinities is of importance in the reproduction of gender order. The construction of femininity as the protected part is central; hence woman bodies are non-existence in the CSDP (Kronsell, 2016, p. 311). Feminist critique on the traditional view of state and security has elaborated arguments of the link between securitisation and masculinity construction (Ericson, 2018, p. 97). According to it, security is built on patriarchal logic where the man is seen as a protector protecting vulnerable women and children (Enloe, 1990, p. 12). A theory of masculinist protectionism formulated by Iris Marion Young (2003) draws on Foucault's approach of pastoral power. She asserts that already existing mechanisms legitimate paternalistic state powers supported by patriarchal

forms of masculinity in the times of threats. Her theory shows a powerful discursive logic of differentiation between those who need protection and those who can provide it. The tasks are gendered as the protector's position is associated with masculinity. Consequently, the role of being vulnerable and in need of protection is associated with femininity (Young, 2013, p. 13).

Julia Slupska (2019) shows in her smart home security analysis that cybersecurity research does not account in its threat models for domestic and intimate partner violence (IPV). She argues that practitioners and designers will not account for technology as a facilitating factor in abuse if researchers ignore the domestic threat model (Slupska, 2019, p. 84). Slupska also notes that the emerging dynamics of excluding women in international relations seems to repeat in the field of cybersecurity. For example, she highlights the issue of "revenge porn" as non-consensual pornography, which is a gendered technologically-mediated form of abuse. However, cybersecurity experts and practitioners rarely recognise it as a cybersecurity issue. Instead, it is considered as a "privacy issue". To strengthen her argument, Slupska notes that when confidential information is shared with unauthorised third party in the business world, it is certainly classified as a cybersecurity issue. It is also shown that who designs and codes matter and consequently has consequences if it is only a narrow section of society designing and building technologies that are widely used. To emphasise this, she introduces Google search algorithms that converted into sexist and racist because they echo the values and biases of the persons who design and create them (Slupska, 2019, p. 87).

The simple question "where are the women in global politics" has been asked by the feminist scholar Cynthia Enloe (Enloe, 1990). Sjoberg (2015) answers with a simple resolution: "Women are everywhere. They constitute just more than half of the population of the world". Sjoberg then explains that Enloe's question is about women's non-existence in narratives of essential details concerning war and conflict in global politics. After all, if women are half of the world's population, why are they not included in conversations concerning wars and conflicts? (Sjoberg, 2015, p. 437) If women were half of the people using cyberspace, why are they overlooked in cybersecurity policies and their security in cyberspace?

4. Feminist theory

International security, in theory, and practice, remains in several ways a man's world (Tickner, 1997, p. 628). Regarding the number of women in privileged positions in international security and policymaking, women's appearance in these positions is still rare. Patriarchal norms are, in many ways, presence in practice and theory of international security. Therefore, feminism has had a hard time achieving a severe role in security studies (Sjoberg, 2009b, p. 184).

However, according to feminist theorists in international relations, gender is a relevant factor when addressing and understanding different kinds of security issues (Sjoberg, 2009b; Ellerby, 2013; Tickner, 1997). In many ways, the contemporary feminist theory rejects the positivist idea that the world is directly accessible to the researcher. In contrast, knowledge about the world is seen as socially constructed. Therefore, a researcher must always examine neutrality and objectivity of spoken language (Tickner, 1992, p. 36). According to Jill Steans (1998), feminism in international relations is: "*to look at the world through gendered lenses is to focus on gender as a particular kind of power relation, or to trace out how gender is central to understanding international processes*" (Steans, 1998, p. 5). Characters of masculinity and femininity are the base for social hierarchies, and gender symbolises them. Therefore, this gendered social hierarchy is socially constructed and remains to shape our world (Sjoberg, 2009b, p. 187; Wadley, 2009, p. 39).

Moreover, to understand and explain international security issues, the patriarchal hierarchy must be recognised. Binaries of personal/political and internal/external violence have been challenged by feminist IR theorists showing that threats to women's security are ignored or diminished. Unfortunately, these insights have not been incorporated into the emerging field of cybersecurity, resulting in neglecting women's safety once again. Therefore, a feminist approach to cybersecurity must be human-centric, focusing on humans' harm (Slupska, 2019, p. 84).

4.1 Securitization and de-securitization

This theory draws upon the Copenhagen School's rendering of security. The Copenhagen school framework is known for its widened security agenda. It can be associated as a part of a larger assembly of critical approaches to rethinking the traditional security concept. The view of security studies in the Copenhagen school is particularly focused on the importance of

language and power relationships to security concepts. In this approach, security is connected to politics and power structures. Securitising actors construct this view of security by a "speech act". For threats and vulnerabilities to count as security issues, they need to differentiate from the political normative and be spoken out by a securitising actor. A speech act is a process of naming and constructing a threat toward a protected object - the referent object of security - and is often done by an individual group such as the government, leaders or military groups. In the process of securitising, the securitised issue becomes prioritised above "normal politics" (Buzan, 1997 & Mackenzie, 2010). According to Ole Wæver (1995), when a problem is securitised, it tends to lead to particular ways to address it. The threat, defence and solutions are often state-centred. By contrast, de-securitisation is the process when a problem is intentionally left out of the agenda and therefore, de-securitised (Wæver, 1995, p. 65).

Feminist security studies share values with the approach of the Copenhagen School. Both scholars criticise the limitations of the traditional definitions of security and place significant emphasis on language and power relationships (Mackenzie, 2010, p. 204). Lene Hansen (2000), a feminist scholar, has pointed out the non-existence of gender-based insecurity in the Copenhagen school. However, she has emphasised the potential of securitisation to be used in feminist studies (Hansen, 2000, p. 286). This study aims to use the concept of securitisation to analyse what is seen as a security threat in the EU cybersecurity. Moreover, the ambition is to determine if securitisation can explain why human trafficking is overlooked in the EU cybersecurity.

4.2 Poststructural feminism

Poststructural feminism may be defined as a theory in international relations which supports the statement that the distinction between public and private has had significant consequences for women's economic, political and cultural marginalisation. The constructions that women were fragile, irrational, emotional, short-sighted and everyday-oriented and were, therefore, to reside in private, legitimised the distinction between public and private. These understandings of femininity and masculinity were kept in place by the discourses and practices. However, poststructural feminism argues that these constructions can be changed by reworking the political assumptions of gender (Hansen, 2010, p. 23). According to poststructural feminism, gender is performative. It is a "performed" system of meaning within specific historical and cultural boundaries. Moreover, gender is constituted through social interactions (Steans, 2010, p. 75). Poststructural feminist research is concerned with the silences resulting from different

discourses that construct subjects and subject positions. If there is no “woman” subject, either is there “lived experiences” that could be used as statements of what women experience and consequently, needs (Hansen, 2010, p. 24). Moreover, depicting women as “victims” is warned by poststructural feminists as it strengthens the subject position of women being passive or pitied instead of convenient political agents (Hansen, 2010, p. 24; Kronsell, 2006).

4.3 Hegemonic masculinity

Kronsell (2016) studied the European Union's security and defence policy (CSDP) and highlighted that it is male-dominated. However, it is invisible through the process of normalisation. Therefore, I believe that using the theory of hegemonic masculinity to complete this thesis's aim would be suitable because of the close relation between CSDP and the European Union cybersecurity. Kronsell refers to Hearn and Parkers' (2001) statement of "the silent unspoken, not necessarily easily observable, but fundamentally material reality" of institutions. Institutions with hegemonic masculinity have silence on gender as a determining character. Men are the type of normality, what it is to be human or a person. However, it is not written or spelt out (Kronsell, 2006, p. 109). These are the norms that are shaped by exclusively including men and excluding women. Hegemonic masculinity has influenced both policies, agendas and politics of these institutions (Kronsell, 2005, p. 281). According to Kronsell, norms of masculinity don't need to be thematised as they remain to be reproduced by the routines of these institutions (Kronsell, 2005, p. 283)

The predominance of masculinised logics within other security domains (Ericson, 2018; Blanchard, 2014; Kronsell, 2016) and the construction of cyberspace (Deibert, 2018; Dunn Cavelty, 2012), would advocate norms of hegemonic masculinity within the EU's cybersecurity institutions. Poststructural feminism would advocate that the historical distinction between public and private and the understandings of femininity and masculinity have constructed the new domain of cybersecurity. The discourses and practices of masculine logics that have dominated the security field have also transferred to dominate in the emerging field of cybersecurity. The theory of hegemonic masculinity argues that the silence of men being the typical normality has normalised practices to exclude women invisibly. Norms of masculinity remain to be reproduced by the routines of these institutions. However, if opened up to the "other", institutional change and development could happen simultaneously changing gender

relations. In sum, we can presume logics of hegemonic masculinity be found in security and technology and, consequently, influencing cybersecurity practices. In this study, I will focus on this normality that is reproduced within the institution and problematise these unspoken silences and men's hegemony. However, as Kronsell has stated, this can be problematic because masculine norms usually remain hidden when they are hegemonic (Kronsell, 2006, p. 110). How this can be done, according to Kronsell, is to question the obvious by breaking the silence and making the familiar strange.

5. Methodology

The European Union cybersecurity strategy consists of three main action pillars - cybercrime, cyber defence and critical information infrastructure protection which sets out how to respond and prevent cyberattacks and disruptions (Carrapico & Barrinha, 2017, p. 1260). The following five priorities are set out to address different challenges: achieve cyber resilience, drastically reduce cybercrime, develop cyber defence policy and capabilities related to the EU's common security and defence policy, develop the industrial and technological resources for cybersecurity and establish a coherent international cyberspace policy for the EU (Cyberwiser, 2020). By the complex nature of the EU as a cybersecurity actor, this thesis cannot encompass the entire scope of the EU's cybersecurity. Therefore, the analysis will consist of an outline of the EU's cybersecurity and a more in-depth analysis of cybersecurity policies from the European Commission, Europol and ENISA using a feminist security approach.

The focus in the analysis will be how security is expressed in the policies and for whom is it, in the masculinities that can be found written in between the lines, and poststructural understandings of gender norms. The EU cybersecurity strategy is particularly interesting because there are reasons to expect that the EU would consider gender and human trafficking in cybersecurity policies. This thesis's topic – find out why human trafficking is overlooked in the EU cybersecurity – is relatively confined and clearly described. Therefore, an interpretive case study approach is considered suitable. This thesis follows a qualitative case-study, with in-depth analysis of three different hypotheses that will answer why trafficking is overlooked in the EU cybersecurity. Interpretive research is not variable based and traditionally, do not talk about hypotheses. However, an interpretive researcher can develop creative hypotheses to explain unexpected observations that prior theory does not fully explain. In interpretive research, this technique is called abduction (Schwartz-Shea & Yanow, 2012, p. 37). Anyhow, hypotheses that are presented in this thesis are not to test them right or wrong. Preferably, they will be used as a framework for the analysis and limit the topic into explaining through three theories, why human trafficking is overlooked in the EU cybersecurity. This thesis attempts to highlight the problem and to propose possible explanations for the issue. These hypotheses are based on three feminist security approaches: securitisation, hegemonic masculinity and poststructural feminism. The methodological approach taken in this study is a mixed methodology based on textual content-analysis and deconstruction. Moreover, text as an

empirical material is vital to interpretive political analysis and therefore, textual analysis of different cybersecurity policies seemed suitable for this thesis (Mark & Rhodes, 2016, p. 195).

Interpretive research is marked by the ontological assumptions that the world is socially constructed. The focus lies on meanings which shape institutions and actions (Mark & Rhodes, 2016, p. 3l). The data should be treated as an indication of the meanings embedded in actions (Mark & Rhodes, 2016, p. 18). In this thesis, these meanings are embedded in the cybersecurity policies. Central concepts in this study are not defined beforehand. Instead, the definition of central concepts has emerged from the field. As familiar to interpretive research, literature is used to advance researchers prior knowledge (Schwartz-Shea & Yanow, 2012, p. 37). It is essential to bear in mind that this thesis does not want to generalise results. Instead, it attempts to offer possible explanations of an observed phenomenon. However, findings of this study can still have relevance to other contexts even if it may not directly aim generalisability. I am aware that there is a methodological concern of the risk of confirmation bias in this study. However, in interpretive research, when a researcher interprets the data, there is always a risk that the interpretation is biased to support the researcher's hypotheses. Therefore, complete objectivity is impossible to be achieved. However, I have carried these concerns in my mind and completed the analysis guided by the principal of confirmability. The principal of confirmability means that my values or the theoretical biases should not affect the investigation (Bryman, 2012, p. 392-393). I have also aspired to operate upright and transparently present my analysis.

5.1 Deconstructing silences

Deconstruction has been used since the early 1990s by feminist IR researchers to shed light on how mainstream IR field is laced with gender stereotypes, practices and dichotomies while unconscious to gender (Kronsell, 2006, p. 110). According to Kronsell, "*deconstruction makes gender relations visible by overturning the oppositional logic that mystifies categories like woman/man, domestic/international, and peace/war*" (Kronsell, 2006, p. 110). To expose underlying historically derived norms to concepts, double reading of the material is required. Gendered norms in the academic discipline of IR theory have been made visible by the deconstruction method (Kronsell, 2006, p. 111). However, there are differences between academic institutions of IR as well as military and defence institutions. This thesis will not analyse military and defence institutions but a security institution; the European Union. However, I believe that this method can be applied to analyse the EU's cybersecurity as it has

a strong connection to the EU's security. According to Graig Murphy (1998) there is a highly relevant connection between these institutions. He means that the very core of international relations (IR) is the link between the military and men and the exclusion of women from these activities (Murphy, 1998, p. 94). Realism can be categorised as a primary traditional security approach of IR and is a form of embodiment of hegemonic masculinity as elite white men's perspectives to protect the state have been projected onto states' behaviour (Kronsell, 2006, p. 111). In IR practices, such as defence security and military organisations, gender has been silenced.

In other words, when studying silences, the researcher needs to rely on methods of deconstruction. With the technique of deconstruction, the researcher can find conditions that are not included in the text. The researcher has to see what is written between the lines. This technique requires a broadness in the material that is analysed and detailed reading of the texts. Double reading of the material is necessary to provide insights (Kronsell, 2006, p. 115). In order to deconstruct, abduction of the material is necessary in interpretive research. Underlying structures behind a text can be found by moving back and forth in the material. This makes it possible to critically examine the circumstances responsible for the theory. This technique is called retrodictive (Mark & Rhodes, 2016, p. 92). I am aware that this can be a methodological challenge because I am studying something that is not there but hidden in the text. However, deconstruction is a critical aspect of feminist research which I aim to contribute with my thesis (Kronsell, 2006, p. 115). The analysis in this thesis is done by first using a content analysis method to analyse all material chosen for the analysis. The material was carefully read through several times, and each hypothesis was used as a “perspective” or “lens” to identify content relevant to each hypothesis. In other words, the material was read through with three different “lenses” to explore parts that needed to be analysed in-depth. After that, reconstruction was used to analyse the material in order to see the silences behind the text. To determine whether each hypothesis could serve as an explanation or not, the process of deconstruction was repeated several times. Purpose of the analysis was to determine if the hypotheses could be an answer to the question “why is human trafficking overlooked in the European Union cybersecurity?”. At the beginning of each analysis, each hypothesis is explained and based on a theory presented earlier in this thesis.

5.2 Material

The analysis will consist of an outline of the EU's cybersecurity and a more in-depth analysis of data relevant to this study's aim. Choosing text to analyse in a study is by itself an interpretive process. As it is earlier stated, being completely objective in interpretive research is impossible. When a researcher chooses the data, there is always a risk that it is biased to support the researcher's hypotheses (Schwartz-Shea & Yanow, 2012). However, I have kept this in mind when selecting the material for the analysis and considered all the relevant data to choose documents representing the EU cybersecurity in the best way.

The first document chosen for analysis is 2013 *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, which lays out the EU's visions on how to strengthen security in cyberspace and sets out actions needed to accomplish the outlined vision. To complement the analysis of the EU's cybersecurity strategy, the second document chosen for analysis is 2020 *Communication from the Commission on the EU security union strategy*. This document is a communication for a new strategy for 2020-2025 which focuses on building capacities and capabilities to enhance the EU's security environment. The communication defines priorities and actions required to address both digital and physical risks. This document was chosen to understand the contemporary visions as a complement to the original cybersecurity strategy. The third document is the *EU Regulation 2019/881*, generally cited as the Cybersecurity Act. The Act was adopted in April 2019 to strengthen the EU's cybersecurity rules and includes a mandate for the EU's cybersecurity agency ENISA along with the introduction of a European cybersecurity certification framework for digital services, processes and products.

With diving deeper into the threat landscape, two additional documents were chosen for analysis. The first document is ENISA's *year review from January 2019 to April 2020 of the threat landscape*. This document outlines a general overview of the threat landscape and provides ENISA's list of top 15 threats, recommendations and conclusions. The second document turns the gaze towards cybercrime, namely Europol's *Internet organized crime threat assessment 2020* (IOCTA), which aims to connect at the strategic, tactical and operational levels about different cybercrime threats. The document contributes to the 2021 EMPACT prioritizing for operational action plans. The current priorities presented are disrupting criminal activities against information systems, combating child sexual abuse and child sexual exploitation and targeting criminals involved in fraud.

6. Analysis

6.1 Hypothesis 1: Human trafficking is overlooked in the EU cybersecurity because of the non-human referent object of security

The first hypothesis is based on the theory of securitisation. According to Buzan (1997), threat depends on what is seen as a threat to a referent object of security. Therefore, the referent object of security is the object that is being protected by the securitising actor. In this study, the securitising actor is the European Union.

Security in cyberspace depends on who is secured and from whom. What is striking as a tendency in the cybersecurity policies is the focus on obtaining cyberspace as a domain and securing information systems, networks and information and communication technology (ICT). Cybersecurity is defined in the Cyber Security strategy as follows:

> "*Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."*
> (European Commission, 2013, p. 3)

However, on the same page, it is stated that the Cyber Security Strategy "*outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world*" (European Commission, 2013, p. 3). In other words, cybersecurity is defined to include securing the cyber domain from threats that are associated with it at the same time stating that protection and promotion of citizens' rights should be base for all of the actions. The strategy gives the first impression that both the cyber domain and citizens would be referent objects of security. However, there is an inconsistency with the presentations. The inconsistency continues further in the five priorities set up in the strategy which are: "*achieving cyber resilience, drastically reducing cybercrime, developing cyber defence policy and capabilities related to the Common security and defence policy, developing the industrial and technological resources for cybersecurity and establishing a coherent international cyberspace policy for the European Union and promoting core EU values*"

(European Commission, 2013a, p. 5). Security of the cyber domain is strongly present in these priorities, while core EU values are mentioned in the end. The emphasis on non-human referent object of security can furthermore be found in the Cybersecurity act as it proposes to "*improve cybersecurity in the Union so that network and information systems, communications networks, digital products, services and devices used by citizens, organisations and businesses (...) are better protected from cyber threats.*" (Regulation (EU) 2019/881)

Regarding core EU values, democracy, fundamental rights, and the rule of law are repetitive in these different documents. In the Cybersecurity strategy it is stated that "*The EU international engagement in cyber issues will be guided by the EU's core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights."* (European, Commission 2013, p. 15). Furthermore, the communication for a new strategy states that "*The EU can also ensure that security policy remains grounded in our common European values - respecting and upholding the rule of law, equality and fundamental rights and guaranteeing transparency, accountability and democratic control - to give policies the right foundation of trust*." (European Commission, 2020, p. 1). However, the inconsistency lies within the conflict of securing the cyber domain as well as citizens' rights, and what kind of threats are presented as a threat towards cybersecurity. As Buzan (1997) argued, the referent object of security is protected from the danger by a securitising actor. What can be found from the different cybersecurity policies is that the presented threats are threats against non-human objects. Cyber attacks and cybercrime are seen as threats to cybersecurity. Moreover, these threats are presented as attacks; politically motivated, criminal, terrorist, state-sponsored attacks, and unintentional mistakes and natural disasters. On the other hand, cybercrime is stated to be one of the threats against security in cyberspace. Cybercrime is defined as follows:

> "*Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)*" (European Commission 2013, p. 3)

However, the cybercrimes expressed in the Cybersecurity strategy include mostly economic crimes toward information systems for EU governments and companies such as holding companies to ransom, stealing critical data, state-sponsored activities and economic espionage (European Commission, 2013, p. 3). It can also be found in the ENISAs' document of the threat landscape that in 2018 there was a pattern in the view of threats. The activity that was seen as a threat was threats targeting the economy. Threats targeting networks, businesses, the economics of businesses and individuals have continued in 2019-2020 (ENISA, 2020).

In what way threats and insecurities are presented produces different kinds of discourses which gain hegemony over human rights and social policies (Ericson, 2018, p. 96). What stands out from the cybersecurity policies is the silence on gender and the inconsistency of the referent object of security. The existing presentations fail to resolve the contradiction between non-human referent objects and citizens' rights as referent objects. The core EU values and fundamental human rights are repetitively mentioned in the different policies to be the fundamental ground for all actions. However, only a few of the threats mentioned against cybersecurity are threats against these rights. Instead, they are threats towards non-human cyberspace as a domain and objects such as information systems, networks and ICT products. One possible implication of this contradiction could be de-securitisation. Previous research has proposed security to be a process where threats are constructed or de-constructed (Nunes, 2015). In the case of the EU cybersecurity, threats related to non-human objects are constructed and therefore gain hegemony over human rights and social policies. As Hirschauer (2019) showed in her study about sexual violence at the time of post-World War II, active silence was a process of de-securitisation (Hirschauer, 2020, p. 219). In the case of cybersecurity in the EU, the active silence on gender and non-existence of human trafficking in policies could be seen as de-securitisation. By this, I would propose that human trafficking may be de-securitised from the agenda of cybersecurity in the EU. There is an active silence on both gender-related threats in cyberspace and cyber trafficking in the cybersecurity policies in the EU, which makes these threats invisible in the domain. Moreover, this active silence on gender and human trafficking is then normalised by emphasising the core EU values and fundamental rights.

6.2 Hypothesis 2: Human trafficking is overlooked in the European Union cybersecurity because of hegemonic masculinity

The second hypothesis is based on the theory of hegemonic masculinity and previous research on hegemonic masculinity in security institutions. The predominance of masculinised logics within other security domains (Ericson, 2018; Blanchard, 2014; Kronsell, 2016) and the construction of cyberspace, would advocate norms of hegemonic masculinity within the EU's cybersecurity institutions.

It is stated in the Cybersecurity Strategy that there are several stakeholders of the digital world, and many of them are non-governmental and commercial entities. These stakeholders are involved in the management of internet resources, standards, protocols, and the internet's future development (European Commission, 2013, p. 4). According to the European Commission, there is a large gender gap in the digital sector. Only around 17 % of the ICT specialists in Europe are women even though women possess more than half of the European population (European Commission, 2019). Therefore, it is likely to believe that the digital world is male-dominated. In previous research it is also shown that who designs and codes matter (Slupska, 2019). Consequently, it has consequences that it is only a narrow section of a society developing and building widely used technologies. A possible explanation for the silence on gendered issues could be that the representation of women and men in the digital world is unequal. As a result, there is not enough representation to push the gender-related problems to the agenda's top. The European Commission is emphasising more women to be included in the digital world. It endorses that women's participation is crucial to building a sustainable, fair and equitable digital society and economy (European Commission, 2019). However, the current cybersecurity policies seem to be constructed by male domination in the domain. As also noted by Slupska (2019), the emerging dynamics of excluding women in international relations seems to repeat in the field of cybersecurity.

Regardless that the European Union values gender equality, no aspect of gender is mentioned in any of the cybersecurity policies. In the 2013 Cybersecurity Strategy key aspect of focus connected to the cyber defence dimension was to develop EU cyber defence capabilities to address different kinds of capability development. The mentioned aspects are leadership, doctrine, organisation, personnel, training, technology, logistics, infrastructure and interoperability (European Commission, 2013, p. 11). Many different areas are mentioned here, however no aspect of gender. According to critical feminist perspectives, gender-sensitive

security must start with women's everyday experiences and link these experiences with broader political processes and structures (Hudson, 2005). The crucial problem with silence on gender in security discourse is that it will be impossible to secure if it is not considered in the policies. In the EU cybersecurity policies, no lived experiences are consulted. The non-existence of lived experiences has consequences. As Sjoberg (2019) has argued, only by recognising that threats differ between different genders can these threats be fully understood and countered (Sjoberg, 2019).

The analysis of the non-human referent object of security in cyberspace also underpins the analysis of hegemonic masculinity. It is connected to the traditional security approach where the nation-state is always the referent object of security and therefore, protected (Kronsell, 2006). According to Judith Stiehm (1982), the protection consists of different power relationships where the protector has power over those he protects. Therefore protection encompasses control over another object (Stiehm, 1982). In this case, the nation-state as a referent object of security is replaced with cyberspace. It is the one being protected in the EU cybersecurity, which the masculine protector needs to defend. If protection is about control, then cybersecurity in the EU would include control over cyberspace. How protection and control are relevant to the analysis of hegemonic masculinity is indeed the feminist critique on the traditional view of state and security. According to it, there is a link between securitisation, non-human securitisation, and masculinity construction. The concept of security is built on patriarchal logic, where the man is seen as a protector protecting vulnerable women and children (Enloe, 1990, p. 12) Therefore, it is likely that protection and control over cyberspace are gendered and connected to hegemonic masculinity in the European Union. Logics of hegemonic masculinity could explain why gender and human trafficking in cybersecurity are silenced. After all, as Kronsell (2005) has argued, norms of masculinity don't need to be thematised because they remain reproduced by the routines of institutions of hegemonic masculinity.

6.3 Hypothesis 3: Human trafficking is overlooked in the European Union because the issue is seen as a private matter and, therefore, does not belong to cybersecurity.

The third and last hypothesis is based on the theory of poststructural feminism, which supports the statement that the distinction between public and private has had significant consequences for women's economic, political and cultural marginalisation. Because of the construction of femininity as fragile, emotional and vulnerable, women were to reside in the private (Hansen, 2010, p. 23). Poststructural feminist research is concerned with silences that are consequences from different discourses that construct subjects and subject positions. If there is no "woman" subject, either is there "lived experiences" that could be used as statements of what women experience and consequently, needs (Hansen, 2010, p. 24)

As noted in previous sections of this analysis, gender does not play a vital role in the EU cybersecurity policies. The word "gender" and "woman" are mentioned only a couple of times in all cybersecurity documents. In the Communication for a new strategy, gender is mentioned in the section where public spaces' protection is expressed. It is pointed out that: "*An important aspect to reflect is the fact that minorities and vulnerable individuals can be disproportionately affected including persons targeted because of their religion or gender, and therefore require particular attention*" (European Commission, 2020, p. 9). However, it needs to be noted that the quote is from a part where security is expressed in general, not in cyberspace. However, in this analysis, security in public spaces can be drawn to touch the issue with cyberspace too. If it is recognised that individuals can be more vulnerable because of their gender in public areas, why is particular attention not paid in cyberspace? Global computer networks have created a virtual meeting place that allows information sharing and public interaction - cyberspace. According to Lincoln Dahlberg (1998), cyberspace is seen as providing the foundation of democracy and the public sphere (Dahlberg, 1998). Even though there is no consensus of the concept of cyberspace, I would, in similar to Dahlberg, place it to be counted as a public space. A public space builds the majority of cyberspace with some private places such as private chats. Like a city that is mostly a public space for anyone to walk freely, it also contains private areas such as private apartments. Clark (2003) has also identified that environments that are supposed to be safe for women and children such as their families, communities and public places of business and commerce are actually increased risk-zones for them (Clark, 2003, p. 248). Therefore, it could be assumed that gender should be an essential aspect that should also require particular attention when securing cyberspace. However, the EU cyber security fails to take

gender into account, which can explain why human trafficking is overlooked in the EU cybersecurity as it is not seen as a public issue in the cyberspace.

Furthermore, the following is expressed in the Communication for a new strategy: "*Bringing the security of the online and physical environments in line means continued steps in countering illegal content online. More and more, core threats to citizens such as terrorism, extremism or child sexual abuse rely on the digital environment: this calls for concrete action and a framework to ensure respect for fundamental rights.*" (European Commission, 2020, p. 13) In the first sentence, illegal content is mentioned to be a threat which needs to be countered. However, the second sentence excludes human trafficking from the issue. Terrorism, extremism and child sexual abuse are mentioned as core threats to citizens as they rely on the digital environment. When expressing issues about illegal content, how can it be possible that such a large problem as human trafficking is not taken into consideration in Communication for a new security strategy? Latonero (2012) conducted a research about technologically enabled human trafficking in 2012 and already then highlighted that the marketing of victims sold for the purpose of sexual exploitation is happening online. Moreover, technology allows traffickers to contact large audiences of "buyers" across geographic boundaries and long distances (Latonero, 2012, p. 10). Therefore, it is worrying that advertising victims of human trafficking on the internet is not seen as "illegal content" in the Communication for a new security strategy in the European Union.

In ENISA's document of the threat landscape, sextortion is named as a threat. Besides, ENISA expects teenagers and young adults to be targeted by cyber offenders with sextortion attacks in the future as well (ENISA, 2020, p. 15). Sextortion is a form of blackmail where the victim is blackmailed with sexual information or images to extort sexual favours. Sextortion can be put in the same broad category of sexual exploitation. However, in Europol's internet organised crime threat assessment, sextortion is presented as a crime related to money and cryptocurrencies, not as a violation of human rights (IOCTA, 2020, p. 17). Is it possible that this kind of gendered problem (human trafficking) related to intimate violence and exploitation is seen as a private problem and therefore, do not belong to the field of cybersecurity? Slupska (2019) highlighted in her study that cybersecurity experts and practitioners rarely recognise non-consensual pornography as a cybersecurity issue. This gendered technologically-mediated form of abuse is instead considered as a "privacy issue". On the contrary, sharing confidential information with unauthorised third parties in the business world is undoubtedly classified as a

cybersecurity issue (Slupska, 2019, p. 87). Can it be that the current security policies in cybersecurity are constructed from the old understandings of femininity and masculinity, and the distinction between public and private and, consequently, gendered issues are seen as privacy issues in cybersecurity?

However, the theory of poststructural feminism does not fully explain why child sexual exploitation is seen as a cybersecurity issue, and adult sexual exploitation is not. A new strategy to step up the fight against child sexual abuse emphasises tackling child sexual abuse online (European Commission, 2020, p. 13). Furthermore, according to the Cybersecurity act, children must be seen as particularly "vulnerable persons" (Regulation (EU) 2019/881). Inconsistency with the problematisation stands in contrast to the analysis of the non-human referent object of security in cyberspace and the analysis of technologically-mediated forms of abuse as a "privacy issue". However, as it is stated in the Cybersecurity act, children are universally seen as particularly vulnerable and therefore, need protection. Thus, the moral necessity of protecting children can explain why child-related issues are considered even in cybersecurity despite the conflict between referent objects of security.

7. Discussion

7.1 Limitations

The major limitation of this study is the scope of master's level thesis. Therefore, this thesis could not encompass the entire scope of the EU's cybersecurity. This thesis has engaged with policies that I believe represent the EU's cybersecurity well. Therefore, I am aware that there are policies that engage with other concerns related to the cyber field more generally which are not analysed in this thesis. Another issue that was not addressed in this study was changes over time. Policy documents analysed in this study were published between 2013 and 2020. However, investigating changes over time was not the ambition of this study.

7.2 Conclusions

In this thesis, I analysed the EU's cybersecurity to find out possible explanations for why human trafficking is overlooked in the field. Human rights are in the heart of the European Union. Indeed, the European Union is based on a commitment to value fundamental human rights for EU citizens. Furthermore, combatting human trafficking is one of the EU's top priorities. However, the issue of human trafficking is non-existence in the EU's cybersecurity policies. The globalisation and new information technologies have expanded criminals capacity to traffick human beings. Moreover, the internet is an essential part of traffickers' method of working. Therefore, it could be assumed that the issue of human trafficking would be present in cybersecurity policies.

My thesis's purpose was to investigate if feminist security approach could explain why human trafficking is overlooked in the EU cybersecurity. The most prominent finding to emerge from this study is that gender blindness seems to repeat in the emerging field of cybersecurity. This study has also shown that feminist security approach can offer different explanations of why human trafficking is ignored in cybersecurity. Three hypotheses were created from three theories to explain the issue:

- Hypothesis 1: Human trafficking is overlooked in the European Union cybersecurity because of the non-human referent object of security.
- Hypothesis 2: Human trafficking is overlooked in the European Union cybersecurity because of hegemonic masculinity.

- Hypothesis 3: Human trafficking is overlooked in the European Union because the issue is seen as a private matter and, therefore, do not belong to cybersecurity.

With the securitisation theory, I identified that the first hypothesis could explain the issue. In the EU cybersecurity, threats related to non-human objects are constructed and gain hegemony over human rights and social policies. Therefore, threats toward non-human objects are prioritised over threats toward humans, such as human trafficking. The analysis also showed that the active silence on gender and non-existence of human trafficking in cybersecurity policies could be seen as de-securitisation. There is an active silence on both gender-related threats in cyberspace and cyber trafficking in the cybersecurity policies in the EU, which makes these threats invisible in the domain. Moreover, this active silence on gender and human trafficking is then normalised by emphasising the core EU values and fundamental rights.
With the theory of hegemonic masculinity, I identified that the second hypothesis could also explain why human trafficking is overlooked in the EU cybersecurity. The results of this investigation showed that it is likely that protection and control over cyberspace are gendered and connected to hegemonic masculinity in the European Union. Logics of hegemonic masculinity could therefore explain why gender and human trafficking in cybersecurity are silenced. The theory of poststructural feminism supported the third hypothesis that human trafficking is seen as a private issue and therefore, does not belong to the field of cybersecurity. However, the theory does not fully explain why child sexual exploitation is seen as a cybersecurity issue, and adult sexual exploitation is not. With these theories, I was able to identify different explanations for the problem. However, I would assert that they also complete each other and strengthen the resolutions if used together.
I want to emphasise that this study is explorative, and therefore, there could be several other reasons and explanations of why human trafficking is not included in the EU cybersecurity. However, my purpose was to highlight the matter and raise awareness of the gender blindness in the EU cybersecurity and the connection between it and human trafficking. With this exploratory thesis, I can contribute to the cybersecurity scholarship that is lacking feminist research.

One of the most significant finding to emerge from this study is that human trafficking is not seen as a threat to cybersecurity in the EU. The internet is an essential part of traffickers' working method, which is acknowledged by many private tech companies such as Global Emancipation Network and Thorn. These private tech companies aim to build technology to

fight human trafficking in the cyberspace (Thorn, 2020; Global Emancipation Network, 2020). Moreover, the United Nations Global Initiative to fight human trafficking has acknowledged the link between the internet and human trafficking in 2008 (UN.GIFT, 2008). Finally, already in 2002, a group of specialists in the Council of Europe researched on "the impact of new information technologies on trafficking in human beings for the purpose of sexual exploitation" and identified that the sex industry and the internet industry are closely intertwined (Council of Europe, 2002). Therefore, this thesis can be an eye-opener for this issue in the EU cybersecurity institutions. However, it needs to be noted that Europol's executive director Catherine de Bolle declared in October 2020 that: "Human traffickers are using increasingly modern communication technologies to exploit their victims multiple times over: from advertising and recruiting victims, to blackmailing them with photos and videos to control their movements. To counter this threat, we have to use the great advantage of shared intelligence and collect more digital evidence." (Europol, 2020) The future will show, if human trafficking will be recognized as an issue also in the EU cybersecurity.

This thesis's final contribution is to generate policy suggestions related to the problem presented in this study. The results of this study suggest that to create safe cyberspace from human trafficking cybersecurity policies should:

- Start from women's everyday experiences
- Asses that threats are different for women and men in the cyberspace
- Acknowledge patriarchal norms in the cyberspace
- The European Union should establish partnerships with different private tech companies to combat human trafficking in the cyberspace.
- And lastly, to acknowledge human trafficking as a threat in the cyberspace

This study contributes to our understanding of the issue of gender blindness in different fields. In international security, silence toward gender becomes exaggerated, which we can identify in analysing the EU's cybersecurity policies. The challenge is to shape attitudes, policies and laws to protect victims of human trafficking in ways that also preserve rights of expression and freedom.

Lastly, I would like to advocate that further feminist research of cybersecurity should be conducted. The scope of this thesis has limited further investigations on how policymakers and stakeholders see this problem. Therefore, such research with interviews, with policymakers and stakeholders, would provide a more profound knowledge of this phenomenon. It would also be particularly interesting to compare different international organisations with the EU to see if human trafficking is included in the cybersecurity policies. Moreover, different countries could be compared in the same matter to see if the problem is better combatted at a state-level.

Literature

Bevir, M & R.A.W. Rhodes. (2016). Interpretive Political Science: Mapping the field. In Bevir M. and R.A.W. Rhodes, eds. *Routledge Handbook of Interpretive Political Science*, pp. 3-29. London; New York: Routledge.

Blanchard, E. (2014). Rethinking International Security: Masculinity in World Politics. *The Brown Journal of World Affairs.* 21(1): 61-79. DOI: 130.242.58.169

Bryman, A. (2012). Social research methods. 4th ed. Oxford: Oxford University Press.

Buzan, B. (1997). "Rethinking Security after the Cold War", *Cooperation and Conflict* 32(1): 5-28.

Carrapico, H. and Barrinha A. (2017). The EU as a Coherent (Cyber)Security Actor? *Journal of Common Market Studies 55*(6), 1254-1272.

Clark. M. A. (2003) Trafficking in Persons: An issue of human security. *Journal of Human Development*, 4(2):247-263, doi: 10.1080/1464988032000087578

Council of Europe. (2002). Group of specialist on the impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation. (EG-S-NT). Final report. https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/group_of_specialists_on_the_impact_of_the_use_of_new_information_technologies_1.pdf (Accessed: 13-10-2020)

Dahlberg, L. (1998) Cyberspace and the Public Sphere: Exploring the Democratic Potential of the Net. *Convergence*, 4(1):70-84. doi:10.1177/135485659800400108

Deibert, R. (2018). Trajectories for Future Cybersecurity Research. In Gheciu, A. and Wohlforth, W. (eds.) 2018. *The Oxford Handbook of International Security*. Oxford. Oxford University Press.

Dunn Cavelty, M. (2012). The Militarisation of Cyberspace: Why Less May Be Better. In C. Czosseck, R. Ottis and K. Ziolkowski (eds.), *2012 4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE, 141-153.

Ellerby, K. (2013). (En)gendered Security? The Complexities of Women's Inclusion in Peace Processes. *International Interactions.* 39(4), pp.435–460. doi: 10.1080/03050629.2013.805130

Enloe, C. H. (1990). Bananas, beaches and bases: Making feminist sense of international politics. London: University of California Press.

Ericson, M. (2018). "Sweden Has Been Naïve": Nationalism, Protectionism and Securitisation in Response to the Refugee Crisis of 2015. *Social Inclusion, 6*(4), 95-102.

European Institute for Gender Equality. (2018). Gender-specific measures in anti-trafficking actions. Report. Luxembourg. *Publications office of the European Union*. https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/read_the_report_gender-specific_measures_in_anti-trafficking_actions.pdf (Accessed 13-10-2020)

Europol. 2020. The challenges of countering human trafficking in the digital era. October 2020.

Greiman, V. Bain, C. (2013). The emergence of cyber activity as a gateway for human trafficking. Journal of information warfare. Yorktown. 12(2): 41-49.

Hansen, L. (2000) The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School, *Millennium: Journal of International*

Hansen, L. (2010). Ontologies, Epistemologies, Methodologies. In Shepherd L. (ed.) 2010. *Gender matters in global politics. A feminist introduction to international relations.* New York. Routledge. (17-27).

Hirschauer, S. (2020). De-securitization, sexual violence, and the politics of silence. *European journal of women's studies.* 27(3). 219-234. doi: 10.1177/1350506819889379

Hudson, H. (2005). 'Doing' Security As Though Humans Matter: A Feminist Perspective on Gender and the Politics of Human Security. *Security Dialogue, 36*(2), 155-174.

Hughes, D. (2014). Trafficking in Human Beings in the European Union: Gender, Sexual Exploitation, and Digital Communication Technologies. *SAGE Open*. 4(4), 1-8. doi:10.1177/2158244014553585

Nunes, J. (2015) Emancipation and the reality of security. In: Balzacq, T. (ed.) *Contesting Security: Strategies and Logics*. New York: Routledge, 141–153.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International security.* 38(2): 7-40

Kronsell, A. *(2006)* Methods for studying silences; Gender analysis in institutions of hegemonic masculinities*, 108*-128. in Ackerly,B. Stern, M. and True, J. (eds.) *Feminist methodologies for international relations.* 2006. Cambridge. Cambridge University press.

Kronsell, A. (2005) Gendered practices in institutions of hegemonic masculinity*, International Feminist Journal of Politics.* 7(2): 280-298. doi: 10.1080/14616740500065170

Kronsell, A. 2016. Sexed bodies and military masculinities: Gender path dependence in EU's common security and defence policy. *Men and masculinities*. 19(3): 311-336 doi: 10.1177/1097184X15583906

Latonero, M. (2011). Human trafficking online: The role of social networking sites and online classifieds. *Center on Communication Leadership and Policy*. University of Southern California. Retrieved from https://technologyandtraf-ficking. usc.edu/files/2011/09/HumanTrafficking_FINAL.pdf

Liaropoulos, A. (2015). A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia. *Journal of Information Warfare.* Yorktown. 14(4): 15-24.

Lobasz, J. (2009). Beyond border security: Feminist approaches to human trafficking. *Security studies*. 18(2): 319-344. doi: 10.1080/09636410902900020

Mackenzie, M. (2010) Securitizing Sex? Towards a theory of the utulity of wartime sexual violence. *International Feminist Journal of Politics*. 12(2): 202-221. doi: 10.1080/14616741003665250

Murphy, C. (1998). Six Masculine Roles in International Relations and Their Interconnection: A Personal Investigation. In *The 'Man' Questionin International Relations*. Zalewski, M. Parpart, J (eds.). Boulder: Westview Press, 93–108

Schwartz-Shea, P. & Yanow, D. (2012). Interpretive Research Design. Concepts and Processes. New York, NY: *Routledge*.

Sjoberg, L. (2009) Introduction to Security Studies: Feminist Contributions. *Security Studies*. 18(2): 183-213. doi: 10.1080/09636410902900129

Sjoberg, L. (2015). Seeing sex, gender, and sexuality in international security. *International Journal.* 70(3): 434-453. doi: 10.1177/0020702015584590

Slupska, J. (2019) Safe at Home: Towards a Feminist Critique of Cybersecurity. *St Antony's International Review.* 15(1): 83-100.

Steans, J. (1998) Gender and International Relations: An Introduction. New Brunswick, NJ. *Rutgers University Press*.

Stiehm, J. (1982). The Protected, the Protector, the Defender. *Women's Studies International Forum. 5*(3): 367-376.

Tickner J. (1992). Gender in International Relations: Feminist Perspectives on Achieving Global Security. New York. *Columbia University Press*.

Tickner, A. (1997). You Just Don't Understand: Troubled Engagements Between Feminists and IR Theorists. *International Studies Quarterly* 41(4):611–32.

Thakor, M., Boyd, D. (2013). Networked trafficking: reflections on technology and the anti-trafficking movement. *Dialectical anthropology*. 37(2): 277-290.
doi: 10.1007/s10624-012-9286-6

UN.GIFT. (2008). United Nations Global Initiative to fight human trafficking. Background paper. Workshop 017. Technology and human trafficking. https://www.unodc.org/documents/human-trafficking/2008/BP017TechnologyandHumanTrafficking.pdf (Accessed: 13-10-2020)

Pettman, J. (1997). Body politics: international sex tourism. *Third world quarterly*. 18(1): 93-108.

Young, I. M. (2003). The logic of masculinist protection: Reflections on the current security state. *Journal of Women in Culture and Society*. *29*(1):1–25.

Wadley, J. (2009). Gendering the state, Performativity and protection in international security. In Sjoberg, L. (ed.) *Gender and international security: Feminist perspectives*. New York. Routledge.

Wæver, O. (1995) Securitization and Desecuritization. In Lipschutz, R. (ed.) *On Security*. New York: Columbia University Press, 46-86.

Internet sources:

Cyberwiser. (2020). *EU cyber security strategy: An open, safe and secure cyberspace*. https://www.cyberwiser.eu/content/eu-cyber-security-strategy-open-safe-and-secure-cyberspace (Accessed 5-11-2020)

European Commission. (2018). *Data collection on trafficking in human beings in the EU*. Lancaster University and European Commission. doi:10.2837/193237 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20181204_data-collection-study.pdf (Accessed: 29-10-2020)

European Commission. (2019). *Women in digital*. https://ec.europa.eu/digital-single-market/en/news/women-digital (Accessed: 10-12-2020)

European Commission. (2020). *Trafficking in human beings*. Trafficking in human beings (Accessed: 3-12-2020)

European Institute for gender equality. (2018). *Trafficking for sexual exploitation: a gendered crime*. https://eige.europa.eu/news/trafficking-sexual-exploitation-gendered-crime (Accessed: 15-10-2020)

European Union. (2020). *Human rights and democracy*. https://europa.eu/european-union/topics/human-rights_en (Accessed: 15-10-2020)

Glaser. E. (2019). Invisible Women by Caroline Criado Perez – a world designed for men. *The Guardian.* 28 feb. https://www.theguardian.com/books/2019/feb/28/invisible-women-by-caroline-criado-perez-review (Accessed: 1-10-2020)

Global Emancipation Network. (2020). *About.* https://www.globalemancipation.ngo/global-emancipation-network-mission-offerings/ (Accessed: 2-1-2021)

Thorn. (2020). *About us*. https://www.thorn.org/about-our-fight-against-sexual-exploitation-of-children/ (Accessed: 2-1-2021)

Empirical material

Enisa. (2020). The year in review. *ENISA threat landscape*. https://www.enisa.europa.eu/publications/year-in-review (Accessed 11-11-2020)

European Commission (2013). *EU cyber security strategy: An open, safe and secure cyberspace*. JOIN (2013). 01 Final. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf (Accessed: 10-11-2020)

European Commission. (2020). *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the regions on the EU Security Union Strategy*. COM(2020) 605 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605 (Accessed 10-11-2020)

Europol. (2020). Internet organised crime threat assessment. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 (Accessed 10-11-2020)

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN* (Accessed 10-11-2020)