Faculty of Economics, Law and Social Science

# Women, Peace and Cybersecurity

## Widening the Security Discourse by bringing Cybersecurity into the UN Women, Peace and Security Agenda

Department of International Relations
Bachelor Thesis
Mentor: Prof. Dr. Oliver Kessler

Clara Winkler
clara.winkler@uni-erfurt.de
6th semester, Bachelor of International Relations
Matriculation Number: 42419
Summer Semester 2020
Deadline: 15 July 2020

# Content

# 1. Introduction

Women are 27 percent more likely than men to get harassed online (Sharland & Smith, 2019, 29). Cyberstalking has found its way into abuse strategies, as over thousands of German men currently have installed spyware on the phone of their partner to surveil and stalk them (Locker & Hoppenstedt, 2017). Every year "representatives of half the population are being forced to rescind their democratic participation because of rape and [online] death threats" (Walker, 2020, p. 9). – All of those facts sound shocking, but they have been known for quite some time. Despite that, there exists almost no literature by scientific researchers that targets the problem of the security of women in cyberspace. On the other hand, there has been a lot written in feminist security studies on how to redefine the traditional security term promoted by Realists[1] in order to make visible the security threats to which women are exposed every single day.

To fill this gap of literature I will make the link between feminist security studies and cybersecurity in my bachelor thesis. To limit the scope of this paper I will mainly concentrate on binding international law that exists concerning this topic. My research will mainly focus on actions of the UNSC because as it is the only institution of the UN which is able to adopt binding International Law, it is also this institution which is of relevance when redefining the UN's definition of security. There are two problems that I want to tackle: First, major legal institutions in International Law like the United Nations Security Council (UNSC) when talking about women's security actually reinforce gender inequality. And second, the most famous cyberattacks until now cannot be classified as an attack in International Law (IL). Both renders International Law incapable of solving issues of cybersecurity and women's security. I argue that the root of those two problems is the same: *Militarism*. The concept of Militarism is constituted by a set of beliefs like considering only the security of nation states as 'real' security, the exclusive focus on physical force, the framing of men as protectors of women or the belief in hierarchies of command as the nature of society (Enloe, 2016a, p. 11). Through militarized norms, thoughts and systems the number of threats that will count as real security threats is strongly limited. I will demonstrate that e.g. through this strong promotion of *gender stereotypes*, Militarism can and is already leading to a strong discrimination of women, to the incapability to deal with cyber threats and to the combination of both. As those problems cannot be classified within the current term of security which dominates International Law, those

[1] The main subjects of security in Realism are states and political strength is determined by the strength of their militaries. In the theory states are regarded as black boxes, rendering domestic policy and the private sphere unimportant for International Relations. Further elaboration on the realist view of security can be found in Waltz (2018).

resulting problems remain invisible even though they might lead to as serious damages as traditional security threats like a war between two nations.

To support my argument and to find a solution for this problem, I will mainly focus on the first binding international legal document that links the term security to women – the Women, Peace and Security Agenda (WPS Agenda). Consisting of ten United Nations Security Council Resolutions (UNSCR) – last two adopted in 2019 – the WPS Agenda, through focusing on gender related difference in witnessing violence and participating in peace and security, values women's perspectives on conflict situations and promotes the input of women in peacebuilding. I will uncover the Militarism which is still inherent in the agenda despite its goal of promoting women's rights. Next to that, I will elaborate on the status of cybersecurity in International Law and consider the current developments, the problem of militarized norms and some major changes which are being discussed at the moment. This will lead to a better understanding of how to improve the incorporation of cybersecurity into a legal framework. Subsequently, I will demonstrate that an inclusion of this topic into the WPS Agenda has also a great potential to bring real *gender equality* into it. I will use my analysis of the Militarism dominating the WPS Agenda and international legal norms to come up with concrete suggestions on what can be changed in the agenda to overcome Militarism and to ensure cybersecurity for women.

Suggestions for a further development of the agenda are very urgent and topical at the moment as a new resolution is about to be passed. The next resolution is extremely important, because there is a risk that some countries achieve to make the agenda vaguer and therefore ineffective. For feminists it is important that the opposite happens, thus making the agenda more progressive than ever before. The agenda is definitely a milestone as it "presents women, a non-traditional security concern, as relevant to a traditional security body on the world stage, the Security Council" (Hudson, 2010, p. 45), but it is also heavily criticized. Feminists have argued that it is so inherently militarized and unsuited to tackle *gender injustices*, that a "revival of a radical WPS [is] practically impossible" (Shepherd & Kirby, 2016, p. 391). Its 20$^{th}$ anniversary this year is an excellent occasion to reflect on that resolution and its future development and chances to influence or even change the still prevailing understanding of traditional security. I argue that further work on the WPS Agenda towards a demilitarized agenda is still very important as the agenda brought and still has the chance to bring important changes.

In the latest resolution UNSCR 2493 (2019) on Women, Peace and Security the UNSC requests the Secretary General to include "recommendations to address new and emerging challenges"

(UNSCR 2493, 2019, Art. 10 Lit. a) into his annual report. Through working at the intersection of cybersecurity and the global suppression of women, I will exactly work on one of the challenges that are emerging to the WPS Agenda. I develop my argument that the current way security is practiced in international policies is not suited neither for *gender equality* nor for cybersecurity. It is not only that the traditional security vocabulary is not grasping most cyber threats in general, but also that women are differently affected by cyber threats than men and that their issues remain mostly ignored in the current male-dominated cybersecurity field. The topicality of cybersecurity gives an exceptional opportunity to widen the whole security discourse of the WPS Agenda. In my research, I show how emerging challenges like cyber threats make the current problems of militarized traditional security more obvious and therefore have the potential to push the agenda further. The focus on women and cybersecurity in the next resolution of the WPS Agenda could significantly shift the discourse, making it generally more just and inclusive and treating women as subjects, rather than objects.

After a short introduction into ground-laying concepts used in this work, the problem about women and cybersecurity will be outlined. Then it will be argued why the WPS Agenda is significant for this problem. Afterwards certain language issues of traditional security studies will be pointed out, which are problematic in both the WPS Agenda and in cybersecurity. Finally, it will be showed which changes need to be made to solve those issues and how a focus on cybersecurity could help with that.

# 2. The Two Main Concepts: Gender and Cybersecurity

Before I will start to examine the intersection of women and cybersecurity, it is necessary to introduce certain concepts and definitions that will be used throughout this thesis.

Two concepts that will be central in this research that are interacting and shaping the concept of Militarism are *gender* and *gender analysis*. As Wright puts it "feminists have argued that patriarchal gender norms, combined with other global structures such as capitalism, racism and coloniality, play a role in causing […] militarism and war" (Wright, 2019, p. 4).

Gender can be defined as "a system of symbolic meaning that creates social hierarchies based on perceived associations with masculine and feminine characteristics" (Sjoberg & Via, 2010, p. 3). It is not related to the biological sex but represents a way of socialization according to particular norms being attributed to either masculinity or femininity. Gender can be understood as a set of discourses which is transformative and can be perceived differently by diverse individuals and vary due to geographical and cultural location (Sjoberg & Via, 2010, p. 4). The ideas of feminist constructivism and feminist poststructuralism will be dominant in this thesis to analyze the role of gender. The first is focusing "on the ways that ideas about gender shape and are shaped by global politics" (Sjoberg & Via, 2010, p. 3), but with the help of feminist poststructuralism I will also do a linguistic analysis of the UNSCR 1325 to examine "how gendered linguistic manifestations of meaning, particularly strong/weak, rational/emotional, and public/private dichotomies, serve to empower the masculine, marginalize the feminine, and constitute global politics" (Sjoberg & Via, 2010, p. 3). Both theoretical approaches will be helpful to uncover gendered dynamics shaping realities in the WPS Agenda and in cyberspace.

The definition of the term cybersecurity which I found especially suiting for this work construes cybersecurity as "[t]he state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this" (Oxford University Press, 2014). In this definition, systems and humans both can be in the state of protection thus being subjects of cybersecurity. Besides the existing of other definitions[2] that focus exclusively on the protection of "software, computers and networks" (Amoroso, 2007), the one I chose is important for my work because I am focusing on the on the security of women in cyberspace, thus concentrating on the security of humans through the security of systems. Even though there have been certain

[2] Find an extensive analysis of different definitions of cybersecurity in Craigen et al. (2014).

cyber incidents that reached international attention like the cases in 2008 in Georgia[3] and Lithuania[4], none of them qualified as a cyber war and therefore a focus on 'war' in cyberspace is only a minor matter (Mills, 2010). Thus, cybercrime as a more extensive concept, including all "crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism" (Syed et al., 2019, p. 2) is the most important threat faced by the concept of cybersecurity.

In this work I do not only want to look at cybersecurity as stand-alone-subject but put the topic in a wider perspective of what certain elements of cybersecurity mean to international security and the WPS Agenda in general. International security which formerly related "to the threat or use of force by states" (Fierke, 2015, p. 1) with a strong focus on militaries and nation states, has been broadened with the rise of critical security studies, which strive for redefining security. Feminists for example have argued that "[r]ecognising gender as a significant dimension of identity and security opens the door to non-state-based views of security and aptly illustrates how identity shapes individual and collective security needs" (Hoogensen & Rottem, 2004, p. 156). However, official bodies that shape international law still stick to the first definition, also called *traditional security vocabulary* in this work. It will be shown how this still limits the UNSC's dealing with 'non-traditional' security topics like women's rights and cybersecurity.

[3] A massive cyberattack against pro-Georgian websites was launched between July and August 2008 in context of the Russo-Georgian War.

[4] On June 28, 2008 a cyber operation was launched against Lithuania, targeting and taking down administrational and private websites and instead showing communist symbols on the sites. The attack appeared in reaction to a ban of communist symbols by the Lithuanian Parliament (Linaki (2014, p. 173).

# 3. Women Working in and Threatened by Cybersecurity

To exactly understand the representation problems and different discriminations of women in cybersecurity it is helpful to analyze the current situation and the discourse around the topic. There are two types of arguments being made, which will be analyzed in the following chapter.

## 3.1. The Instrumental Argument

The cybersecurity work field is currently very male dominated with different studies saying that 80% (Morgan, 2019) to 89% (Frost & Sullivan, 2013, p. 4) of workers in the sector are men. Different institutions and companies try to change that. The arguments in favor of including more women into something are often of instrumental nature (Hudson, 2010, p. 45). Accordingly, when talking about women in the security sector there exists an often cited study, that peace lasts longer, when women are included in the negotiation process (Krause & Williams, 1997). But for women in cybersecurity such a study cannot be found, thus the instrumental arguments for having more women in in that field are different. Hence, I am now having a look at the leading organizations and companies and their arguments for having more women.

The leading cybersecurity company Palo Alto Networks[5] states in its news blog that "[e]very single country struggles with the shortfall of cybersecurity professionals. […] To overcome this shortage, we need to bring in more women in cyber and diversified skill sets" (Matsubara, 2017). Statements like these are problematic because they contain the underlying assumption that if there would not be such an economic demand of professionals, there would be no need to include women.

Another common instrumental argument made, pleading for more women in the cybersecurity sector is the one of diversity. As WiCys argues, "[i]t also makes perfect sense to hire women into these jobs, because it's been proven that workforce diversity improves productivity and also enhances external perceptions." (Women in CyberSecurity [WiCyS], 2019). The last phrase of this statement seems to suggest that women are just an accessory that looks good to the outside. WiCys is a network NGO bringing together women working in cybersecurity and companies. The fact, that even an NGO promoting women's participation and claims to support women, argues in that way is alarming. It shows that the discourse around women in

[5] Palo Alto Networks was listed 8th in the Forbes ranking of companies that shape the digital economy after i.a. Amazon and Netflix in 2018 (Forbes Press Releases, 2018).

cybersecurity has been pushed far in a wrong direction of not putting women in high positions because of their competences but because it looks good, thus not acknowledging their qualifications. Neither those leading companies in cybersecurity, nor the NGO for women in cybersecurity came to the conviction that women could just have the right to decide about regulations and develop new technologies, that are not privileging men, but are also fitting their needs.

An interviewee of Hudson aptly sums up this dilemma between the instrumental and the rights-based argument:

> *Instrumental arguments are the only arguments that work with policy-makers. Nobody is interested in women because it is the right thing to do or because it's about human rights – nobody. And that's the best reason for working on gender in any area – just because it is right. We shouldn't have to make everything contingent upon positive social development or democratic or peace consequences. It's just right, but that just so doesn't wash. So, yes, instrumental arguments are very important. (Hudson, 2010, p. 46)*

Even though the instrumental argument is highly problematic, and it should always be reflected upon, it can also be helpful when it comes to policy making. Even if certain rulings only come into place, due to instrumental arguments, in the moment a norm comes into force this transforms the discourse into a rights based one, because the topic suddenly becomes a question of rights and legality.

## 3.2. The Rights-Based Argument

Nevertheless, it is also possible to effectively argue in front of policy makers for the necessity for more women in cybersecurity using a rights-based argument. This type of argument is a normative claim, which can be found e.g. in the preamble of the UN-Charter, stating

> *We the people of the United Nations [are] determined to reaffirm faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small. (UN-Charter, 1945, Preamble)*

A rights-based reasoning for women in cybersecurity should highlight that women are differently affected and structurally discriminated by the cybersecurity sector. Women represent around 50% of the world's population (The World Bank, 2018) and therefore they

have the right to be represented in all decision making processes, because they are just as concerned as men. Additionally, norms are meant to be general and target the whole society. Whether intentionally or not, they primarily respond to the needs of males, because historically the system was made to serve them (Criado-Perez & Singh, 2020, pp. 11–16). As the system structurally makes life harder for women it is quite reasonable to develop specific policies responding to the needs and challenges of women. This argumentation is extremely rare because it goes deeper than the instrumental argument. It questions the fundament of our society: patriarchy (Reardon & Hans, 2019, p. 14).

In the following section, there will be given some examples on the systematic suppression of women in cyberspace, which are threatening their security. They highlight the rising complexity of security threats as technology develops further but not in a neutral way. Furthermore, it needs to be emphasized that all discriminations of the female gender can cross with other kinds discrimination. These crossovers and a consequent intensification of discrimination are called *intersectionalism* which need to be considered when doing a feminist research. At that intersection of forms of discrimination, we find e.g. that white women can be more privileged than black women, and a transgender person from an academic background could be privileged compared to a transgender with low education. The first example points right into this.

Because it is developed by humans with particular worldviews, focuses and blind spots technology is not neutral. Increasing representation of women also means reducing bias against them, because they are more likely to see problems which the female gender predominantly faces. The problem of bias becomes apparent e.g. in Artificial Intelligence (AI). One of those gender biased technologies can be found in biometric technologies. Those transform the human body into data. This can be used e.g. for photo tagging, or photo summaries in apps like Facebook, electronic passport checking at airports, for access in public transport and other means, that require electronic facial recognition (Browne, 2015, p. 111). A study researching on “face gender classification on consumer images in a multiethnic environment” (Gao & Ai, 2009, p. 169), finds that when the system is programmed to recognize “all ethnicities”, it often wrongly classifies black women as male and Asian men as female, “mirroring earlier pseudo-scientific racist and sexist discourse that sought to define racial and gendered categories […] to regulate those artificial boundaries that could never be fully maintained” (Browne, 2015, p. 111). This false classification can apart from reinforcing sexist and racial stereotypes, also lead to very bad consequences in real life, in cases where e.g. the police gets a photo from a

surveillance camera and searches a database with faces to find a possible perpetrator. A wrong attribution because of the biased technology can lead to criminal prosecutions of the wrong person. Besides face recognition it was also found that "voice and speech recognition systems performed worse for women than for men" (Gomez, 2019). Adding on to the problem comes the notion of technologies as being inerrant and having a "mathematical precision" (Browne, 2015, p. 115). This creates the impression, that technologies and their developers have a "politically and normatively neutral agenda" (Hansen & Nissenbaum, 2009, p. 1167) as programmers are mostly seen as experts and clearly differentiated from politicians. The biases of people that develop the technology are too often not taken into consideration. It is therefore highly needed to let people of different genders and ethnicities take part into the development to minimize biases of a uniform group as much as possible.

The Australian Policy Institute in its annual series on women peace and security which in 2019 focused on emerging challenges to the WPS Agenda, points out several women's issues regarding security and cyber. As one of the first challenges it mentions the extreme imbalance of women becoming victims of online harassment, the likelihood being 27 times higher than for men (Sharland & Smith, 2019, 29). Cyber violence against women can especially target female decision makers (Sharland & Smith, 2019, p. 28) and also play a dangerous role in violent domestic environments. In domestic violence, which is a recognized violation of human rights (The Advocates for Human Rights, 2012), "technology acts as a less visible enabler for domestic abuse" (Sharland & Smith, 2019, p. 29). The British newspaper *The conversation* puts the problem in a heading "Technology-facilitated abuse: the new breed of domestic violence" (Al-Alosi, 2017). The article shows, how domestic abusers use technology to track their victims, send them abusive messages or blackmail them with private pictures and data. A concrete example is the app FlexiSpy, one of lots of spywares which is used by over thousands of Germans to surveil and stalk their partners, 80% of the perpetrators being men (Locker & Hoppenstedt, 2017). This form of *gender-based violence* has become part of everyday life of many women (Köver, 2019). The victim is robbed of their complete privacy and even if they find out about their total surveillance, few is done against the perpetrator by the state, even though the act is illegal (Köver, 2019). Domestic violence is highly gendered[6] and therefore an inherent structural problem in society, which appears in all parts of the world (World Health

[6] For example in Germany, 50.4% of all victims of murder and homicide, assault, sexual assault, sexual coercion, rape, threat, stalking, coercion, deprivation of liberty, pimping and forced prostitution lived together with their partner, who also was the perpetrator, and in 80.2% of the cases, the perpetrator was a man doing harm to a woman (Bundeskriminalamt (2018, p. 9).

Organization, 2013). The facts that show that technology is used much more against women than men worldwide and makes violence against them easier, make it a highly relevant issue, when talking about the security of women on an international level. Especially when national governments fail to address the problem like e.g. in Germany where there is no law targeting cyber abuse (Deutscher Bundestag, 2016) despite the existence of alarming studies (Amnesty International, 2017) and the high request of NGOs (bff, 2017, p. 13).

Furthermore, technology also facilitates the open suppression of women's rights. An often-mentioned case is the launching of the mobile app Absher by the Saudi Arabian government. The male guardianship law in the country intensely restricts the lives of women and makes them obliged to seek permission of their male custodian for travels, applying for a passport, get married and many other things (Human Rights Watch, 2020). Apart from other government services, the app also has the function for the guardian to give or withdraw those permissions for the women under his supervision online (Sharland & Smith, 2019, p. 29). What on the one hand can be practical to the system, is also very questionable as it allows further bullying of women, as permissions can be withdrawn so easily. Not only the Saudi Arabian government but also Apple and Google have been highly criticized, for offering this app in their app stores and therefore helping to operate it (Sharland & Smith, 2019, p. 29). Anyway, the app works still on their services. Thus, those international companies are complicit in severe violations of women's rights. This case shows, how the effective suppression of women can be enhanced through the development of technology and huge tech firms that are not taking women's lives seriously.

All of those cases can be used to support the rights-based argument, because they show the inherent disadvantaging of women in cyberspace by a global patriarchal system. Stressing those examples and continuously making the rights-based argumentation shifts the discourse much more towards a gender equal world, than just letting them participate because the economy needs them. A rights-based reasoning focuses on equity and makes a reasonable point with its normative claim, that all humans, no matter which gender, should have and be able to exercise equal rights in their lives.

# 4. Significance of the WPS Agenda to Cybersecurity

After having demonstrated the inherent dangers in cyberspace faced by women and stressed the importance of a rights-based argumentation strategy, I will now show why the WPS Agenda is the right tool for achieving gender equality for women and strengthening the rights-based argument. Moreover, I will locate cybersecurity in the WPS Agenda and determine how an incorporation of this topic could push the agenda further.

## 4.1. Women's Security as an International Matter

As was shown, activities in cyberspace can highly threaten the security of women. Gendered (cyber) violence is also not 'just a national issue', but rather a "global epidemic" (Johnson-Freese, 2019, p. 96), resulting from patriarchy being deeply inscribed in most of the world's societies. Nevertheless, women's security and "gender equality issues have been considered as part of a social justice agenda, rather than a power and security agenda" too long, even though a focus on gender-relations reveals highly relevant power structures (Johnson-Freese, 2019, pp. 21–22). The passing of UNSCR 1325 on 31 October 2000 was extraordinarily meaningful, because the UN used their most effective tool – a Security Council resolution, which is legally binding to all members of the UN – to deal with gender affairs. It was the first resolution of the UN Security Council on a gender issue and remains a milestone, as UNSCR 1325 "presents women, a non-traditional security concern, as relevant to a traditional security body on the world stage, the Security Council" (Hudson, 2010, p. 45). Until now there have been added nine further resolutions to the Women, Peace and Security agenda, the last one concluded by the UNSCR in 2019. They all stand on the four pillars of

1. equal participation of women in decision-making processes,
2. applying a gender perspective to events in and around armed conflicts,
3. protection of women's rights and reporting on gender-based violence and
4. support in relief and recovery through medical care

(NATO Review, 2017).

The agenda makes a link between women and the security field, that was seldomly made before outside the feminist field. In that regard, the WPS Agenda really had the power to change the discourse around women and security issues by including the necessary language for the first time. "From October 2000 to August 2008 […] 33 percent, of country-specific Security Council resolutions include language on women and gender. The number of resolutions even mentioning women prior to 2000 is negligible" (Hudson, 2010, pp. 47–48). Furthermore, the

resolutions have also a significant impact on the UN Department of Peacekeeping Operations (DPKO) practices. They led to the regular establishment of gender affairs offices in DPKO missions, gender training for the DPKO staff, the involvement of more women in peace processes, the reporting of gender-specific data and therefore the systematic inclusion of gender-based security concerns (Hudson, 2010, 55, 58). Additionally, the backlash and attention regarding the agenda led more feminists and other scholars to research on topics around women and security. Critically reflecting current frameworks, they made concrete suggestions on how a gender-perspective on security could look like, which led e.g. to the introduction of a feminist foreign policy in Sweden (Vogelstein, 2019), Canada and Mexico (Thompson, 2020). The WPS Agenda also affects national security agendas to the extent, that many countries have developed national action plans to include a gender perspective in their defense and peace operations. For instance, the German government in its national action plan to implement UNSCR 1325 decided on the "introduction of a comprehensive gender perspective in the preparation and further training of Bundeswehr and Federal Police forces" (Bundesregierung, 2017, p. 6). It can be doubted that such a crucial step against gender discrimination in those militarized and male-dominated institutions would have taken place without the WPS Agenda.

## 4.2. The Emerging International Challenge of Cybersecurity

Cybersecurity is relevant to the WPS Agenda as in its latest resolution UNSCR 2493 (2019), the United Nations requests the Secretary General to include "recommendations to address new and emerging challenges" (UNSCR 2493, 2019, Art. 10 Lit. a) into his annual report. Back in 2000, cybersecurity was not yet an important part of the security discourse. Cyberspace only became increasingly securitized with the attacks on Estonia and Georgia and with the increase in online crime, especially the theft of identities and bank details and the following institutional developments e.g. the establishment of the NATO Cooperative Cyber Defence Centre of Excellence in 2008 (Hansen & Nissenbaum, 2009, p. 1157).

Now cyber is an acknowledged part of the security discourse (Hansen & Nissenbaum, 2009, p. 1157) and plays a significant role in suppressing and discriminating women. It also has global importance and seldomly stops at national borders. I therefore argue, that it should at all costs be included in the 'emerging challenges' that the UNSC should deal with in its next resolution on women, peace and security to have an international legal instrument ensuring the respect for women's human rights not only in the material world but also in cyberspace.

The topic needs special attention in the future work of the UNSC notably because there has not been done anything to tackle it yet. Until now there seems to be a blind spot of WPS literature towards cybersecurity as there are few scholars like Poster (2018a) and Sharland and Smith (2019) that deal with women and the effects of that field on them explicitly. The UN don't seem to give much attention to it neither. In the Global Study on the Implementation of Security Council resolution 1325 by UN Women one mention of cyber can be found in the section 'media', mentioning "the rise of cyberbullying" and the global "Take Back the Tech" campaign, which was launched as an "online platform which crowd-sources reports of online threats, harassment and hate speech against women […] in order to show that these incidents are neither isolated nor anomalous, and to advocate for recognition and redress for technology use spurring gender-based violence at the local, national and international levels" (UN Women & Coomaraswamy, 2015, 294, 296). In the last report of the secretary general on Women, Peace and Security, one cyber issue endangering the security of women was mentioned: "In Libya, the United Nations received reports of intimidation, including social media attacks, against women activists and lawmakers" (United Nations Security Council, 2019, p. 12). The UN department which normally deals with cybersecurity is the office on Drugs and Crime. Its Comprehensive Study on Cybercrime mentions gender one time in the sense that around 80 to 95 percent of cybercrime perpetrators are male (United Nations Office on Drugs and Crime, 2013, p. 42). Those are the only three examples of the last years where the UN link women's security and cybersecurity and where it frames this link to be relevant to international politics. The lacking attention of scholars and the UN towards gender-related crime and violence in cyberspace is inappropriate because that type of crime can have as harmful consequences as other forms of violence (further elaboration on this in 5.4.).

There are two points in which cybersecurity and the WPS Agenda can enrich each other to become more inclusive and effective. First, the arguments to include more women in this field by NGOs and companies were mostly instrumental ones. Making it an issue of the WPS Agenda could lead to the significant shift of the argumentation towards a rights-based one. Because even though it were instrumental arguments that motivated decision-makers to the conclusion of the WPS resolutions, through the process of making it a resolution and therefore part of binding International Law, it sharpened the rights of women and created significant leverage for women to participate in the process, just because they have a right to be there. If cybersecurity would be included into that framework, more people would see that the actual reasons for the need of women in cybersecurity are not of economical, but of normative nature.

Second, one of the biggest critics of the WPS Agenda is accusing it of "just trying to make war safe for women" (Wright, 2015, p. 505), which means that it still uses traditional security which is intrinsically patriarchic. But for dealing with cybersecurity a new framework of security vocabulary challenging the traditional security concept, is imperative. This new framework would also enrich the WPS Agenda and effectively address this criticism. If the UNSCR didn't change their security vocabulary when facing a non-traditional security subject for the first time at the creation of UNSCR 1325 in 2000, it gets a second chance now when dealing with cybersecurity through a gendered lens. As the borders between the international and the private increasingly blur through the rising relevance of cyberspace and gender equity and, as through the combination of both, international challenges become more complex, the UNSC needs to adapt its way of defining and dealing with security threats. How that could be done will be subject of the next two chapters.

# 5. The Militarization of Women's issues and Cybersecurity

I just demonstrated why women, due to their affectedness, need international legal standards, criminalizing cybercrimes against them. In the following chapter I will show from a discursive and a legal perspective, how the traditional security vocabulary due to its Militarism fails to effectively deal with women and with cybersecurity and how implementing cybersecurity in the agenda can therefore help to develop new definitions which serve all genders equally.

## 5.1. The problem of Militarism and Gender Equality

Cybersecurity and women have something in common: both cannot be grasped and effectively dealt with by the traditional security vocabulary. However, the United Nations missed that fact, when creating UNSCR 1325. Fortunately, all nations promised to further work on the topic and in the last UNSCR on WPS decided to work on "emerging challenges" (UNSCR 1820, 2008, Art. 10 Lit. a) in the future. The UNSC did not adapt their security vocabulary when facing a non-traditional security subject for the first time in 2000. But it gets a second chance now, when dealing with an emerging challenge like gender perspectives on cybersecurity.

The reason why the traditional security vocabulary is not suited neither for gender issues nor for cybersecurity lies in the fact that this security vocabulary is inherently militarized. Militarism can be defined as "a system of beliefs and practices that regard (preparation for) war as normal and inevitable" (Wright, 2019, p. 4). But what has militarism to do with gender? As militarism "structures a society's understanding of violence through a prism of acceptance of the use of force" (Shepherd, 2016, p. 325), the problem of this system of beliefs is, that it values certain constructions of masculinities, namely those that link manliness to violence and domination, above other masculinities and devalues all femininities under all masculinities (Wright, 2019, p. 4). An agenda that wants to enhance gender equity properly, cannot be built on such a system of beliefs which contains such an inherent gender inequality.

To better understand, how militarization prevents us from reaching gender equity and to see how cybersecurity could help making the flaws of militarization more obvious, in the following section I will dive deeper into ideas of militarization and how they manifest in International Law and definitions of security. It will be shown how this belief system and its manifestations

are inadequate in dealing with cyberthreats as in cyberspace it is much harder to distinguish between masculinities and femininities and gender categories blur increasingly.

## 5.2. Gender Stereotypes and Militarism

In this section gender stereotypes are highlighted and problematized first in the WPS Agenda and then in cyberspace. It will be shown how those stereotypes emerge out of militarized thinking, why they are inaccurate and why it is time to overcome them.

### 5.2.1. The Protector and the Protected

In each resolution of the WPS Agenda the words *protection* and *to protect* appear on average at least seven times. As this concept of protection seems to be common thread running through all resolutions, it is worth to research on what protection means at all and how it is used to reinforce Militarism. Generally, Militarism is based on and evolves out of beliefs and ideas of how our world works. It highly depends on patriarchy and the degradation of anything feminine (Enloe, 2016b). Cynthia Enloe (2016b) crystallized the three beliefs which underly Militarism and which are crucial to the stereotyping of gender. The first belief is that "the world is a dangerous place" (Enloe, 2016b). The second idea is that "human nature is selfish" (Enloe, 2016b). And the third idea is that "men naturally are the protectors of women, who naturally are the protected" (Enloe, 2016b). Those ideas of militarization have a significant impact on the freedom of behavior and movement of people of all genders:

> *If you are categorized as the protected, because you are a child or because you are female or because you are feminized, anyone of those three, then the presumption is, that the protector is the one who has to know a lot about the world, because how else can you be an effective protector. (Enloe, 2016b)*

And if the protectors are the ones who know a lot more about the world, then it will be them, who go out and discover the world and learn even more about their environment, politics and the public's sphere (Enloe, 2016b). The protected meanwhile will stay at home, not move in those wide circles of knowledge, and not gain that important political knowledge (Enloe, 2016b). Consequently, when it comes to fully exercising political rights, women might fail, because the system prevented them from gathering the knowledge and competences to do so (Enloe, 2016b). When the question will be raised, who should carry out important tasks in the public sphere, it will always be men who have more experience in that sphere and therefore

they will get the responsibility for the task (Enloe, 2016b). Thus, the role allocation in protector and protected has "profound ripple effects on who is able to gain political information and therefore […] really can be a full citizen" (Enloe, 2016b). Many gender stereotypes are rooted in the dichotomy of the protector and the protected, like e.g. the prejudice that women are not suited for politics and rather should stay in the private sphere which is reflected by the low number of women in executive or government positions in 2020 (IPU, 2020).

The idea of protection is dominant in the WPS Agenda: the term *protection of women* can be found very often in all resolutions. The UN Security Council seems to have taken responsibility for the protection of women. Therefore, the UNSC sees itself as the protector, which leaves women inevitably as the protected. This role allocation already implicates, which one of them has the wider knowledge and has the right to move in wider circles and who of them doesn't have enough competences to protect themselves. This is reinforced in how the UNSC speaks about women in the WPS resolutions. Analyzing all WPS resolutions together, more than every fourth time the word *women* is mentioned, it appears either as *women and girls* or *women and children*. Thus, directly linking women with minors, therefore emphasizing their alleged *helplessness* (Shepherd, 2008, p. 115). This link of women with minors also makes it seem as if women were *mature* enough to take their own decisions and to protect themselves. The definition of masculinity is directly dependent on that, as in "fixing 'womenandchildren' as the eternally protected, this representation also functions to define men as responsible for protecting 'their' women and children and the nation as a whole" (Shepherd, 2008, p. 119).

With the WPS Agenda, the UNSC does not only want to protect women, but also wants to include women in peace-processes. Unfortunately, with that attempt it only further reinforces militarized stereotypes: The reasoning in the parts of the resolution that promote women's inclusion in peace-processes is not based on the assumption that women should be able to do everything that men do. They are included because they are framed as *peaceful* women and therefore are allowed to take part, but *only* in their peaceful role (Reeves, 2012, p. 353). This manifests a logic of exploitation according to which women are only allowed to participate if they fulfill the characteristics ascribed to them by society. This is exactly, what can be seen as an instrumental argument, which does not lead to gender equity as we have seen. The most effective way to deal with security threats to women, would not be to protect women or to insinuate that all women are generally more peaceful than men. Rather it would be to destroy the mechanisms that suppress their voices and to have women decide which rulings are suiting their demands. It can be concluded that this stereotyping of women arises from militarized

thinking, which must be overcome as quickly as possible so that women, regardless of their characteristics, can participate in international processes with the same rights as men.

### 5.2.2. Gender Categories in Cyberspace

Unfortunately, always when dealing with a new resolution on the WPS Agenda, the UNSC does not acknowledge the shortcoming of its own strategy to genuinely strengthen the role of women. For feminists it already seems obvious (Tamang, 2013; WILPF, 2015; Wright, 2019) but not for the UNSC. Ergo, bringing in a new challenge that makes the problem even more obvious is a reasonable idea. Of course, when fully exercised, this does also include questioning the inherently militarized structures behind the UNSC and the governments taking part in it, that lead to the mentioned ignorance of gender equity issues and stereotypes in the WPS Agenda. But such an analysis would be beyond the scope of this paper. Hence, making the problem more obvious and pointing out the flaws of the UNSC's militarized security vocabulary, is a good starting point. Cybersecurity is excellent for that purpose because it has a feature, that the *real world* does not have – hidden identities. In cybersecurity, categories of gender blur, all actors have very diverse backgrounds, and the threats are extremely diverse. A uniform profile of people dealing with those threats or mindsets using militarized gender stereotypes would rather perpetuate the whole mission. Consequently, cyberspace is a great chance to start getting rid of gender stereotypes and to advance the transformation of social constructions of femininities and masculinities.

Winifred Poster (2018b) argues that "military masculinities are shifting with the onset of the information and network society" (Poster, 2018b, p. 188) as "virtualization enables a proliferation and hybridization of identities" (Poster, 2018b, p. 188). Poster (2018b) gives the example of Shannen Rossmiller, one the FBI's most acknowledged cyber spies. Through taking on a masculine identity in the internet and posing as different terrorists and criminals, she already exposed terror plots and international criminals in over 200 FBI operations (Poster, 2018b, p. 188). By doing that, she deliberately challenges military masculinities, playing with masculinities and femininities through activating them when needed (Poster, 2018b, p. 191). Hence, cyberspace allows people to play with gender stereotypes and societal gender norms, so that individuals that still believe in them or interact according to them with other actors, can easily be tricked.

Militarized gender stereotypes also fall short on the side of hackers. The example of Anonymous, an international hacker group, known for huge cyberattacks and i.a. interaction and data gathering for the WikiLeaks disclosure page, demonstrates that the crossing of cultural and social boundaries is more norm than exception in the hacker community. Gabriella Coleman, an expert on the international hacker group Anonymous describes its members as *tricksters*, characterized by a "burning desire to defy or defile rules, norms, and laws" (Coleman, 2014, p. 34). She argues that stereotypes are often hindering the full understanding of the group's dynamics and actions. While pointing out that several male hackers use female identities and that the organization doesn't lack "key female participants and organizers" (Coleman, 2014, p. 174), she also pleads that "[d]ismantling the stereotypes also allows a greater appreciation of the motivations held by many of these participants. […] This becomes entirely lost if we understand Anonymous through the gross fetish of stereotypes" (Coleman, 2014, p. 175). Statements that there are characterizing common identity properties of the Anonymous participants like the *hacker cliché* are explicitly rejected by her:

> *[I]f we assume the default hacker and geek is generally male, middle-class, libertarian, and white, then it is much easier to treat a hacker's political interventions as juvenile and suspect—arising from a baseline of teenage angst, instead of the desire for politically conscientious action. (Coleman, 2014, pp. 175–176)*

That quote shows, what upholding gender stereotypes and militarized world views could lead to in the worst case: Misjudging the motivations of those carrying out cyberattacks, leading to the underestimation and wrong understanding of cyber threats, just because the perpetrators appear not physically violent or none-male. Avoiding those mistakes is crucial as a small misjudgment could easily lead to cyberattacks with devastating consequences. Additionally, it is necessary to abandon the framing of women as victims or *the protected*, because the most effective way to make cyberspace safe for women would be to have them develop technologies fitting their needs and to give women the prerogative of interpretation on which activities in cyberspace endanger their security. If the WPS Agenda decided to include cybersecurity in its next resolution, it could not do so without challenging its own gender stereotypes to ensure that cybersecurity threats do neither endanger women's security nor the security of whole infrastructures, data, etc.

To conclude this section, the following can be summarized: Militarized thinking, which is prevalent both in current international security policy and in International Law, leads to

stereotyping of gender. Therefore, women are misrepresented, which is why the WPS Agenda does not lead to actual gender equality. Next to that, there are new security threats posed by cyberspace. Stereotyping prevents those security threats, which affect women more than men, from being effectively combated. Demilitarized thinking and deconstruction of these stereotypes could therefore lead to more cybersecurity overall and for women in particular.

## 5.3. Conflict and Post-conflict settings

In this section, further research and elaboration will be done on the context of International Law in which the WPS Agenda and legal norms on cybersecurity are applicable. I will show, that the criterion of armed conflict is limiting the legal protection in face of security threats.

### 5.3.1. Armed Conflict – A Dominant Criterion in International Humanitarian Law

The WPS Agenda has several problems with its militarized definition of violence, one of them rooted in the distinction between conflict and non-conflict situations. To solve the inherent inequalities in the WPS Agenda and International Law it is necessary to look deeper into what *armed conflict* exactly means and what it implicates. The WPS Agenda condemns rape – but only in circumstances of conflict or post-conflict environment (UNSCR 1889, 2009, Art. 3). It acknowledges, that there are threats especially threatening to women – but only if those threats are part of a war tactic (UNSCR 1820, 2008, Art. 1). The WPS Agenda managed to shift the discourse around security threats to women from the classification as individual security threats, towards framing women as collectively threatened. But it keeps being caught by traditional criteria of security that it tries to escape. Violence as a security threat to women is only condemned by the UN if happening in conflict or post-conflict settings. That raises the question, why there exists this distinction between violence in connection with armed conflict and violence without an armed conflict? As most violence against women happens in the private sphere, I argue that the UNSC should bindingly condemn this global systematic suppression of women, regardless of whether there is an armed conflict around it or not. Through only focusing on post- or armed conflict situations "[r]ather than creating space for greater debate on the many different conditions of inequality within which women (and, in some cases men) often negotiate sex, the debate is foreclosed by a resort to the classic trope of war as a site of male violence and female submission" (Grewal, 2015, p. 156). If determining the gravity and consequences of violence against women, it makes no sense to distinguish whether it happened during what the UN define as armed conflict, other types of conflict or no conflict at all, if the violent act

remains the same. The criterion of whether military force is involved in the situation should not be decisive on whether violence against women is taken seriously. This is big sign of the militarization of the WPS Agenda and International Law.

The criterion of armed conflict plays such an important role in the agenda because of a principle of International Humanitarian Law (IHL), which is only applicable in situations of armed conflicts (Schmitt, 2011, p. 89). This category from international humanitarian law generally takes up too much space in all international law and hardly allows for international legal control in times of peace. This is reinforced by the responsibility of UN Security Council that pursues the mission of maintaining "international peace and security" (UN-Charter, 1945, Art. 1 Para. 1) and foremost focuses on conflict and conflict prevention. The sticking point here is that the terms and definitions of "international peace and security" (UN-Charter, 1945, Art. 1 Para. 1) the UNSC uses come from the UN-Charter, which contains an understanding of the international community and its conflicts from 1945. At that time, the understanding of nation states as the only actors on international level, and an international system based on the Westphalian peace were still dominant. But International Law is always developing further, jurisprudence gets challenged and changed over time. The inappropriateness of focusing on armed conflict in IL is becoming increasingly apparent, while feminist issues are becoming more pressing and new issues such as cybersecurity rise in relevance.

### 5.3.2. No Arms in Cyberspace? – The Unarmed Conflict

If the impropriety of the criterion of armed conflict is not obvious enough when talking about violence against women in general, it will lead to additional problems when it comes to cybersecurity. The problem of this narrow definition of conflict is crucial to why it will be such an important challenge to include cybersecurity into the agenda. The focus on armed conflict leaves huge question marks when dealing with cyberspace. What is the arm in a cyberwar? Is the internet an arm? Or a computer? Or is there just no arm and therefore no need for international legal ruling in those cases? Scholars of International Law showed that they have serious doubts on whether some cyber-attacks can be grasped by IL at all (Linaki, 2014; Schmitt, 2011). To see where cybersecurity can be located in IL, specifically in IHL, I need to dive deeper into the definition of armed conflict.

The framework of application of International Humanitarian Law is its goal to regulate conflict and not to prohibit it. Even though no one was considering cyberattacks during the drafting of

the first Geneva Convention 1864, which is in the core of IHL, scholars and jurisprudence developed definitions and strategies on how to apply IHL to conflicts in cyberspace. An armed conflict needs to fulfill two criteria to be determined as such – the first one being the involvement of *armed forces*, which for cyber operations is the case when they "amount to a cyber-attack" (Linaki, 2014, p. 171). In traditional war, " '[a]ttacks' means acts of violence against the adversary, whether in offence or in defence" (Protocol I, 1977, Art. 49 Para. 1), with *acts of violence* referring to physical violence (Linaki, 2014, p. 170). Thus, certain highly militarized parts of the actual law have to be bypassed through legal interpretation to even grasp cybersecurity, because "it has been acknowledged that the term 'acts of violence' denotes physical force and 'combat action', but within the context of cyberoperations there is no physical clash of armed forces" (Linaki, 2014, p. 170). Subsequently, to classify a cyber operation as a cyberattack, one must concentrate on the consequences of the attack and not, like in the analysis of every other attack, on its nature. A cyber operation is classified as a cyberattack when resulting "in damage or destruction of an object, injury or death of persons or the cause of serious illness or severe mental suffering. […] [T]he duration of the conflict and the amount of killing are irrelevant to the determination on the existence of a conflict" (Linaki, 2014, p. 171). The conclusion of looking at cyber operations and only considering its consequences and not how it was carried out, leaves no space to distinguish between physical and non-physical violence anymore. Why that is important to note, will be explained in chapter 5.4.

However, a cyberattack is not enough for the application of IHL, it needs to result in an armed conflict. Therefore, next to the involvement of armed forces, there either has to be state involvement (leading to an International Armed Conflict) or "the participation of an organized armed group and a certain level of intensity" (Linaki, 2014, p. 172) (leading to a Non-International Armed Conflict). Both can be hardly found in any cyber-attack. To fulfill the criterion of an organized *armed group*, there need to be found strong order hierarchies like they can be found in the military, which in many loose hacker groups don't exist (Schmitt, 2011, p. 98).

Additionally, proof is needed, that the state with the origin of the cyberattack supported the group (Schmitt, 2011, p. 105). Cyber incidents in the fewest of cases can be traced back to the country of origin, and even if that is possible, it is likely that it is a wrong track intended by the perpetrators (Linaki, 2014, p. 175). State attribution in IL is one of the most important criteria. Even though in most cases of violence against women no state attribution can be found, the

WPS Agenda explicitly mentions only situations in and around armed conflicts, which often request state attribution. Thus, the resolution puts a certain barrier of relevance of violence against women in place, namely when it is attributable to a state or a recognized conflicting party. Feminists have argued for a long time that viewing international relations from a state's perspective is strongly biased and doesn't allow researchers to gain a comprehensive understanding of international relations which have "derived from a social and political context where masculine hegemony has been institutionalized" (True, 2005, p. 247). If we did not have the criterion of state attribution, suddenly a lot more conflicts could be recognized on the international stage, on which the UN could act, like many more cyberthreats and also the collective threat of men to women in the private sphere. Both kinds of threat don't happen in the framework of interstate conflicts but feminists have argued that they are just as relevant (Shepherd, 2008; Tickner, 1997).

The cyberattacks that were of the most concern for our current international system like Lithuania and Georgia are not fitting the definitions of an *armed attack* because they are not clearly attributable to a state and did not affect nor lead to military operations (Linaki, 2014; Schmitt, 2011). Therefore, IL is inapplicable, even though there is an obvious conflict, which needs ruling. International Law does not reflect that serious security threats can evolve from cyberspace, as it has not effective measures to deal with such threats.

Taking a closer look, the main problem of the term armed conflict and its incapability to deal with gender issues and cyber issues is its inherent Militarism. The criterion of armed conflict asks for a strong hierarchy, armed forces and state attribution for a conflict to be classified as internationally relevant in traditional security vocabulary. This leaves out a lot of conflicts, which are as relevant to the world's population like e.g. cyberattacks or the systematic suppression of 50 percent of human lives. Also, other increasing security threats like terrorism have problems with being classified as armed conflicts (O'Connell, 2008). If that term does not lose its importance, International Law risks becoming more and more ineffective with the rising importance of other conflict forms than the traditional state-military-against-state-military war. Taking into consideration that the amount of affected are irrelevant to the juristic constitution of a conflict (Linaki, 2014, p. 171), if the criterion of state attribution and the link to military armed forces were to be left out of the definition of conflict, chances would be high that domestic violence against women would also fall in the category where IHL is applicable. Like for cybersecurity it should count for gender-based violence that the criterion of *act of violence* only focuses on the consequences of the action being "injury or death of persons or the cause

of serious illness or severe mental suffering" (Linaki, 2014, p. 171) and not require 'physical violence'. Then even structural violence against women could be legally prosecuted with the help of International Law. To continue on that note, further points on the definition of violence will be elaborated in the next chapter.

## 5.4. Taking All Forms of Violence Serious

This chapter demonstrates that violence in International Relations and International Law is used in a biased way which leads to limited applicability of International Law when it comes to not only cybersecurity but also to security threats against women. It will be shown that the acknowledgement of only certain forms of violence is rooted in Militarism and can lead to serious consequences.

### 5.4.1. The Recognition of Violence against Women

> *The "understanding of violence, as constitutive of subjectivity, has historically been absented from academic theorizing of security, where violence is conventionally conceived of as a functional mechanism within an anarchic international system. […] I seek to understand the types of body that are marked and made through violence that is specifically gendered – that is, violence that 'emerges from a profound desire to keep the binary order of gender natural or necessary'" (Shepherd, 2008, p. 2)*

The former UN Special Rapporteur on Violence against Women and Special Representative of the Secretary-General on Children and Armed Conflict analyzed the beginnings of the discourse around women and violence quite accurately: "Until the 1990s, violence against women was a taboo subject, and only issues involving discrimination primarily in the workplace and in the family were discussed at the international level" (Coomaraswamy, 2014, p. 53). We came a far way since then, but all acknowledgement of violence against women is the result of hard fights of women's organizations and feminists – the patriarchic world system did not recognize any women's issues only because it was 'just' to do so. Taking into consideration that 30 years ago problematizing violence against women on the international stage was a taboo, contextualizes the adoption of the UNSCR 1325 ten years later. Only seven years earlier, in 1993, the UN Human Rights Conference in Vienna recognized women's rights as human rights. That historical context shows that the adoption of the Women, Peace and Security agenda only stands at the start of the development of recognizing women's rights and the violations of these rights.

The development did not stand still as more resolutions on the agenda were passed, but a true change regarding which parts of violence against women are seen by the international systems and which ones are invisibilized, did not take place. All WPS resolutions acknowledge violence against women and equal participation, an understanding of international conflict and violence dating back to the establishment of the UN-Charter in 1945. But with the rising importance of non-traditional security issues like women and cyber which do not fit into that understanding and the resulting definitions, the UN-Charter loses more and more of its topicality every day. The consequence of such international agreements missing new developments was already seen several times in human history. Due to a lack of further development, the Hague Conventions of 1899 and 1907 was followed by World War I and later the League of Nations failed, because its lack of assertiveness had not been tackled and this resulted in World War II.

One of the developments the UNSC is missing is now is the outdating of its definition of violence. As was shown in 5.3., violence in IL is originally defined as physical violence. This already starts to change, because when dealing with cyberattacks, jurisprudence is only concentrating on the consequences of the violent action being "damage or deconstruction of an object, injury or death of persons or the cause of serious illness or severe mental suffering" (Linaki, 2014, p. 171). Furthermore in 2019, the UN acknowledged an insufficient international legal strategy to deal with cybersecurity in its General Assembly Resolution on "Countering the use of information and communications technologies for criminal purpose" (A/RES/74/247, 2019, p. 2), with emphasizing

> *the importance of the international and regional instruments in the fight against cybercrime and the ongoing efforts to examine options to strengthen existing and propose new national and international legal or other responses to the use of information and communications technologies for criminal purposes. (A/RES/74/247, 2019, p. 2)*

This shows that IL and even the UN slowly move away from the current definition of violence, leaving space to discuss the term anew. Security and violence are linked in the sense that security can be broadly understood as the "absence of violence" (Molutsi, 2000, p. 180). Given that "[m]any IR feminists define security broadly in multidimensional and multilevel terms—as the diminution of all forms of violence, including physical, structural, and ecological" (Tickner, 1997, p. 624), the question can be raised, why a UNSCR, that explicitly focuses on women's security, only takes into account physical violence against women and not psychological and structural violence. Like in cybersecurity, for women's issues it is also

necessary to not hold on to the definition of physical violence but to concentrate on the consequences of the action.

### 5.4.2. Structural and Psychological Violence

The agenda sets a focus against rape, defined as sexual violence, but never mentions structural violence like the curtailment of abortion and reproductive rights, even though people can die because of rape and because of unprofessional abortion.[7] Concerning the curtailment of women's reproductive rights, there is no kinetic energy involved, exactly like in cyberattacks. And even though IL, with the according rulings in IHL, does focus on the consequences of cyberattacks, the UNSC does not do the same with security threats to women even though large numbers of women are victims of both. However, to a certain degree the UNSC tackles structural violence – namely the underrepresentation of female staff in peacekeeping missions and security personnel – through pleading for the inclusion of more women. And here the UNSC already become incoherent. This revealing: The UN argue that through the involvement of women, a more stable peace can be reached. Peace as the UNSC uses it, is strongly centered on the absence of conflicts between states (UN-Charter, 1945, Art. 1 Para. 4). Thus, the UNSC pledges for the inclusion of women as long as it serves for the state's security, but it does not go further than that, as it does not acknowledge the problem of gender based violence during what the UNSC defines as peace times. When looking at emerging challenges, cyberspace increasingly gives additional room for structural violence against women. The development of AI is likely to become very misogynist and cyber stalking threatens more women every day, as they remain underrepresented in legislation and technological development processes because of patriarchal power-structures.

Regarding psychological violence, the situation looks even worse. Even though psychological violence is a huge and recognized part of gender-based violence (CETS No. 210 Art. 3 lit. a), no WPS resolution even mentions the word. The only word pointing into this direction is the term 'psychosocial' which in all resolutions together appears exactly seven times and every time in an enumeration of services which should be provided for women, but never in focus. In fact, a focus on psychological violence is urgently needed, because through the further development of technology, women get harassed disproportionately often, while stalking and

[7] Unprofessional abortion is a global problem which caused at least 22,800 deaths internationally in 2014 (Guttmacher Institute, 2018).

other forms of psychological violence become easier for the perpetrator and more untraceable than ever before.

Leaving out of those two types of violence and still desperately clinging to the definition of violence as exclusively physical (Linaki, 2014, p. 170), shows an obvious militarization and preference for male humans. It ignores the two types of violence that are psychological or structural, with at least the last one being more likely to be faced by women than men (Mazurana & McKay, 2001). Therefore, if the UNSC really wants to protect women and their rights, but also if it wants to remain relevant in new emerging fields of conflict, it needs to widen its definition of violence. Certain steps have already been taken by other bodies of the UN, e.g. by recognizing the fight against structural violence against women as essential for achieving the Sustainable Development Goals (Manjoo, 2014, p. 6), but no woman profits from mere lip services. Without the recognition by the main international security body – the UNSC, it will not change that every day, many women worldwide become victims of structural and psychological violence or even die of it.

## 5.5. How to Redefine Security

In this chapter I outline the newest developments of a slow change of the definition of security in the UN system. Drawing on that, I come up with concrete suggestions on what a new definition of security could look like, which can tackle non-traditional security issues like cyberspace and women effectively.

### 5.5.1. Different Understandings of Security

In the previous sections of this chapter, we saw how underlying stereotypes and the selective definitions of the security vocabulary of the UN impede real gender equity throughout the Women, Peace and Security Resolutions. My research allows me to conclude several necessary actions to tackle this: Redefining that vocabulary and abandoning the concept of traditional security itself. In the UN-Charter as in many UN documents, the main goal of the UN "[t]o maintain international peace and security" (UN-Charter, 1945, Art. 1 Para. 1) is mentioned very often even though there is never an official definition of those terms by the UN. However, it becomes clear that in the understanding of the UN, those terms are centered around the state. In the UN-Charter states are clearly set up as the only entities having full legal capacity in International Law as only they can become members of the UN (UN-Charter, 1945, Art. 3, 4)

and only they can call the UNSC (UN-Charter, 1945, Art. 35). Thus, "maintaining international peace and security" (UN-Charter, 1945, Art. 1 Para. 1), at least at the time as the UN-Charter was signed, clearly referred to peace between states and security of states. However, over time the UN also saw a need to act on environmental issues or social justice, for example within the Sustainable Development Goals. As result, the definition of what falls into the maintenance of internationals peace and security broadened. Kofi Annan put it accurately that "[i]n the wake of these conflicts, a new understanding of the concept of security is evolving. Once synonymous with the defence of territory from external attack, the requirements of security today have come to embrace the protection of communities and individuals from internal violence" (Annan, 2000, p. 43). He also acknowledges that "security can no longer be understood in purely military terms" (Annan, 1999, p. 15). However, agendas which contain a broader definition of security like the Agenda 2021 and the Agenda 2030 were adopted by the UN General Assembly. The resolutions adopted by the UNSC show that it still sticks with a state-centered and highly militarized definition of security which focuses on armed conflicts or *post-armed-conflict settings*. That remains the case, probably because in the UNSC the five permanent and therefore most-powerful members can also be found among the six largest arms exporters of the world, together making 73% of the global share of major arms exports (World Economic Forum, 2019). Thus, those are highly militarized states with a still very militarized definition of security, shaping the work of the UNSC whereas the rest of the 193 countries in the world, which are much less militarized, pursue a more human centered security approach in the General Assembly.

### 5.5.2. Flaws of a State-Centered Security Approach

The problem of a state centered approach to security is, that it implies that the state provides a certain level of security to the inhabiting individuals. Thus, only external threats to the construct of a state as such and not threats to individuals within need to be taken as serious security concerns (Hansen & Nissenbaum, 2009, p. 1160). But experience shows us that this assumption is wrong. The security of an individual is not always provided by the state, which can be seen in many cases but maybe most obviously non-white or female humans experiencing systematic racism or sexual violence and discrimination inside of states. If a state focuses on the security of its own construct it might be able to secure its borders or send out its army, but it remains very powerless in the case of a terrorist attack or a cybercrime which are mostly attacks from individuals and loose groups to individuals. One case in 2019 showed the inability of state

actors and media to handle an action, which was done by an 18-year old German citizen. He published data of individuals, that had already been hacked (Zeit Online, 2019). Newspapers like BILD made headlines suspecting Russia behind everything, calling the case a hacker attack. However, when the real perpetrator was found, language immediately changed from the crime of a hacker attack to skimming (ARD, 2019a, 2019b). That conflict, which was wrongfully alleged as of international scope, demonstrates that it does not make sense to attribute conflicts to the states from which the attack is carried out if individual motives lie behind it. This skim was taken very seriously at the beginning but immediately lost importance, when it became clear that it was not carried out by a state, even though the act remained the same. It is also interesting to see, that the interior minister saw the urgency to hold a special press conference and to publicly condemn the action (phoenix, 2019) even though it were only 1000 people whose data had been published – politicians and celebrities. The more than 1000 victims of cyber stalking in Germany (Locker & Hoppenstedt, 2017) are never worth mentioning in any work of the interior ministry.

# 6. Towards the Fall of Patriarchy with the Help of Cybersecurity and WPS

As result of the previous analysis I will make some concrete suggestions on what can be done to demilitarize the WPS Agenda with the help of cybersecurity. However, I will not stop at the WPS Agenda but also tackle the deeper root of militarized UNSC resolutions, which lies in the militarized structures of the UNSC itself, thus raising broader questions for further research.

## 6.1. A Demilitarized Definition of Security

The previous example about the skimming attack in 2018 shows that only attacks on some sorts of individuals seem to be threatening the state's security but not attacks on others (e.g. the 1000 victims of cyber stalking in Germany), even though they count for the same number of people. Here it is worth questioning who is really threatened: Really state security? Or is it rather a collective experience of individuals? If the latter, then both attacks should be of the same relevance. Hansen and Nissenbaum (2009) in their analysis of cybersecurity agree that a state centered approach is not helpful and sum up the complexity of instead centering security around individuals:

> *[T]o articulate security as 'individual security' – as most of Human Security, Critical Security Studies, and Feminist approaches still do – necessitates a collective conception of how and by whom the securities of individuals are going to be negotiated. Since 'individuals' do not appear in political discourse as free-standing entities, but with gendered, racial, religious, class, and other collective identities, there is always going to be a tension between different forms in which the individual can be constituted. (Hansen & Nissenbaum, 2009, p. 1160)*

Feminists have long been working on redefining security and with other emerging challenges like cybersecurity such a redefinition gets more urgent than ever before. Because with traditional security terms the international community is not capable of dealing with any security threats that appear either in the private sphere and/or contain non-kinetic energy, and which are carried out by individuals but nevertheless are affecting lives in the whole world. A new definition of security should therefore concentrate on ensuring the physical and psychological integrity of individuals, not on whether a construct of thought – the state – is concerned. There should be no militarized criteria of physical force or arms for a conflict to be

recognized internationally. There should be no criterion of relevance determined by whether the act is happening in private or public sphere. For determining relevance there rather should be the criterion of a collective experience of a threat, meaning that a certain group of people experiences a certain type of violence. But the definition of violence also needs to be demilitarized, to contain all forms of physical, psychological, structural and non-kinetic harm. There should be no division of humans into protectors and protected and no victimization of the latter. Furthermore, legal texts that deal with security threats should not only concentrate on those that are harmed. Rather, focus on the perpetrators should be included, with the goal of finding all means to prevent the culprits from further exercising their force over others.

With such a demilitarized definition of security, not only inequalities of ethnicity, class and gender can be targeted. Questioning which types of conflicts are taken seriously by the UNSC and the international community, discloses their inherent militarization (Tickner, 2006, p. 24). The rising attention to the negotiation of women's rights and the rising number of cybercrimes, both reaching far beyond national borders, show how outdated a definition of security focusing on states is. With a new definition, it would be possible to deal with all kinds of diverse threats very effectively, which, like cybersecurity, might not fit into the old security vocabulary and definitions. The UN General Assembly might acknowledge that, but as the UN Security Council is the only institution of the UN which is able to adopt binding International Law, it is also this institution which is of relevance when redefining the UN's definition of security. How a new definition of security could be implemented into the UNSC will be examined in the next section.

## 6.2. Demilitarization of the UNSC

> *Reversing a militarizing process […] requires serious rethinking of ideas about femininity and manliness. (Enloe, 2016a, p. 12)*

Demilitarization is a "step by step process" (Enloe, 2016a, p. 12) that "entails making [something] less dependent than it has been on militarized values" (Enloe, 2016a, p. 12), including making something less dependent on fixed gender norms. There are several ways in which demilitarization of the UN in favor of gender equality could take place. The first one points to very drastic ways of reforming the UNSC. With the goal of maintaining "international peace and security" (UN-Charter, 1945, Art. 1 Para. 1) between "nations" (UN-Charter, 1945, Art. 1 Para. 4), which defines a state-centered approach from the beginning on, all resolutions

adopted by the UNSC are moving in the framework given by the UN-Charter. To move away from that, a demilitarized international security that the Security Council is committed to maintain, could be measured e.g. by access to food by the world population or by "how much trust the poorest members of the society have in public officials and their institutions" (Enloe, 2016a, p. 12), simply put by ensuring individual security. To profoundly reform the UNSC towards individual security and to strongly promote equity among all genders, ethnicities and classes a new UN-Charter would have to be written, taking all of this into account. Additionally, some structural amendments of the UN would be needed, to demilitarize decision-making processes and make them more inclusive. The role of non-state actors would need to be strengthened and at the same time, processes that lead to binding international law, like the current UNSCRs, should not be dependent on the most militarized states of the world, like they are at the moment. However, proposals to reform the UN's structure have been around for decades with no result and trying to unite all countries in the world to adopt a new, just UN-Charter sounds like a utopia. Those profound changes would lead to real equality but seem to be extremely difficult to implement and would take a very long time.

The second way to demilitarize the UNSC would be to use the current system as basis and to transform it with the implementation of new concepts. To uncover all ideas of masculinities and femininities underlying the UN system, the UNSC resolutions on Women, Peace and Security are a great starting point, because especially there, the conditions of applicability of IL, limited to armed conflict, is a huge problem. Demilitarization with the help of cybersecurity would mean to start developing a new WPS resolution for the series and include in it the topic of cybersecurity. Because of the missing legal clarity of the conflict-status of cyberthreats and cyber conflicts, including cybersecurity would automatically lead to an obvious discrepancy with the setting of the UNCR 1325 being only conflict and post-conflict situations. Additionally, requests of feminists for a more radical agenda would be reinforced by cybersecurity specialists, that are currently asking to abandon the focus on wars between states and plead for a stronger focus of the security discourse on crime, because that is, what constitutes the most threats to cyber and women at the moment (Mills, 2010). As in cyberspace gender categories increasingly blur in cyberspace, this can also push the UNSC to finally drop their gender stereotypes and abandon their approach to only focus on the role of women by victimizing them, as it is important "to address the social construction of masculinities as a driver of conflict, in order to advance an anti-militarist WPS Agenda with greater focus on conflict prevention" (Wright, 2019, p. 2).

Like all WPS resolution processes before, the whole process for the draft of the new resolution will need a lot of strong advocacy from women's organizations and the will of certain nation states from the UNSC to convince the others. But as the number of NGOs that make the link between women and cybersecurity grows, chances are high that also their advocacy power will grow and therefore they can push towards including cybersecurity in the next resolution of the WPS Agenda. They might even play some of the instrumental arguments that were elaborated in chapter three, because unfortunately it still counts that "[m]ost men will listen if you frame the issue in their terms" (Hudson, 2010, p. 47). However, as soon as a WPS resolution comes into place that promotes gender equity free from stereotypes and Militarism, a new level of leverage will be achieved for all the women in the world fighting for gender justice.

# 7. Conclusion

Throughout this thesis it was shown how enriching a perspective of cybersecurity can be to the WPS Agenda and that it could even lead to major changes in legal standards for women in international law and in the way violence against women is taken seriously by the UNSC.

First, I demonstrated that the incorporation of cybersecurity into the WPS Agenda could change the discourse of why there need to be more women in cybersecurity which at the moment is dominated by instrumental arguments, towards a more rights-based reasoning. Second, the importance and effects of the WPS Agenda on gender equal international security policy were carved out and it was argued that cybersecurity needs to be addressed as an "emerging challenge" (UNSCR 2493, 2019, Art, 10 Lit. a) on which the UNSC wants to work in the future. In the main part of this work, militarism was pointed out as the main reason why the WPS Agenda falls short on reaching real gender equality and why IL cannot deal effectively with conflicts in cyberspace at the moment. It was demonstrated that approaches already exist in International Law, to bypass militaristic criteria such as that of physical violence. Consequently, it was argued that incorporating cybersecurity into the WPS Agenda would be a first step towards demilitarization and real gender equality. It would lead to an obvious discrepancy between the UNSCR 1325's only acknowledging of violence against women in situations related to armed conflict, physical violence with a clear framing of women as victims – and cyberspace, where all those categories are not applicable. Therefore, this process could lead the UNSC to questioning and hopefully dropping those categories. In the final part of this thesis, I suggest that the UNSC should abandon its militarized definition of security and rather act on a definition of security which is characterized by the freedom of individuals from collective threats to ensure their physical and psychological integrity. Furthermore, I draw two visions on how further demilitarization of the UNSC could be realized. Next to the first option of radically transforming the complete UN system, I propose that the more realistic ways is to have the next resolution on WPS, which is going to be passed in the next years, should contain a part that deals with cybersecurity. This can initiate a process that can launch further developments towards true gender equality.

Reviving the WPS Agenda might not be too late at this point, but it will certainly require strong work and will to really change something. However, in the meantime there will still be "state elites [that] – with the help of media editors, academic consultants, technical experts, and husbands – invest a lot of effort in keeping afloat this artificial, unequal relationship between

the masculinized protectors and the feminized protected" (Enloe, 2016a, p. 76). Fortunately, looking at the future, it seems clear that conflicts will appear more and more in a shape which cannot be grasped by the UNSC's traditional security vocabulary and that its work will be outdated sooner or later, if it does not allow internal change towards a more inclusive and human-centered definition of security. Hence, the next WPS resolution is a great chance for the UNSC to slowly adapt its understanding of security in cyber, concerning women and in general. However, changing the definition of security is only the first step into a broader process of demilitarization, which is enabling real gender equity.

Until then, feminists will continue to do research, organizational and activist work in order for the next generation to be free of misogyny in the tech industry, discrimination in artificial intelligence and constant fear of violent attacks – physically or not – against them.

# 8. References


Al-Alosi, H. (2017). *Technology-facilitated abuse: the new breed of domestic violence*. Retrieved April 29, 2020, from https://theconversation.com/technology-facilitated-abuse-the-new-breed-of-domestic-violence-74683.

Amnesty International. (2017, November 20). *Amnesty reveals alarming impact of online abuse against women*. Retrieved July 2, 2020, from https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/.

Amoroso, E. G. (2007). *Cyber security* (1. ed.). Silicon Press.

Annan, K. (1999). Towards a culture of peace. In F. Mayor & R.-P. Droit (Eds.), *Cultures of peace. Letters to future generations: Original texts* (pp. 13–16). Unesco.

Annan, K. (2000). *We the peoples: The role of the United Nations in the 21st century*. United Nations.

ARD. (2019a). *Tagesschau 04.01.2019 20:00 Uhr*. Retrieved July 4, 2019, from https://www.tagesschau.de/multimedia/sendung/ts-29261.html.

ARD. (2019b). *Tagesschau 07.01.2019 20:00 Uhr*. Retrieved July 4, 2019, from https://www.tagesschau.de/multimedia/sendung/ts-29303.html.

bff. (2017). *Fachberatungsstellen und die Digitalisierung geschlechtsspezifischer Gewalt: Ergebnisse einer Umfrage unter Frauenberatungsstellen und Frauennotrufen im bff Berlin, Oktober*. Retrieved July 2, 2020, from https://www.frauen-gegen-gewalt.de/de/aktuelle-studien-und-veroeffentlichungen.html.

Browne, S. (2015). *Dark Matters: On the Surveillance of Blackness*. Duke University Press.

Bundeskriminalamt. (2018). *Partnerschaftsgewalt: Kriminalstatistische Auswertung – Berichtsjahr 2018*.

Bundesregierung. (2017). *Aktionsplan der Bundesregierung zur Umsetzung von Resolution 1325 zu Frauen, Frieden, Sicherheit des Sicherheitsrats der Vereinten Nationen für den Zeitraum 2017 bis 2020*. Retrieved May 5, 2020, from https://www.auswaertiges-

amt.de/blob/216940/dce24ab4dfc29f70fa088ed5363fc479/aktionsplan1325-2017-2020-data.pdf.

Coleman, E. G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso.

Coomaraswamy, R. (2014). Women and Children: The Cutting Edge of International Law. *Proceedings of the ASIL Annual Meeting*, *108*, 43–65.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. http://doi.org/10.22215/timreview/835

Criado-Perez, C., & Singh, S. (2020). *Unsichtbare Frauen: Wie eine von Daten beherrschte Welt die Hälfte der Bevölkerung ignoriert* (Deutsche Erstausgabe, 1. Auflage). *btb*.

Deutscher Bundestag. (2016). *Straftatbestand Cybermobbing: Kurzinformation*. Retrieved July 2, 2020, from https://www.bundestag.de/resource/blob/483622/32b7fb4bb887873dabcbb2b085be08dc/wd-7-154-16-pdf-data.pdf.

Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law applicable in Armed Conflicts. Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (1977). Retrieved July 13, 2020, from https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf.

Enloe, C. H. (2016a). *Globalization and Militarism: Feminists make the link* (Second edition). *Globalization*. Rowman & Littlefield.

Enloe, C. H. (2016b). *'How Can you Tell If You're Becoming Militarized? Doing a Feminist Audit' By Professor Cynthia Enloe*. Retrieved May 13, 2020, from https://www.youtube.com/watch?v=yTuSCKVwGlA.

Fierke, K. M. (2015). *Critical Approaches to International Security* (2. Aufl.). Polity.

Forbes Press Releases. (2018, September 20). *Forbes Releases Digital 100, The Inaugural Ranking Of The Top 100 Public Companies Shaping The Digital Economy*. Retrieved July

2, 2020, from https://www.forbes.com/sites/forbespr/2018/09/20/forbes-releases-digital-100-the-inaugural-ranking-of-the-top-100-public-companies-shaping-the-digital-economy/.

Frost & Sullivan. (2013). *Agents of Change:Women in the Information Security Profession: The (ISC)2 Global Information Security Workforce Subreport*. Retrieved April 28, 2020, from https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2019/03/Women-in-the-Information-Security-Profession-GISWS-Subreport.pdf.

Gao, W. G., & Ai, H. (2009). Face Gender Classification on Consumer Images in a Multiethnic Environment. In M. Tistarelli & M. S. Nixon (Eds.), *Advances in Biometrics* (pp. 169–178). Springer Berlin Heidelberg.

Gomez, E. (2019). *Women in Artificial Intelligence: mitigating the gender bias*. Retrieved April 30, 2020, from https://ec.europa.eu/jrc/communities/en/community/humaint/news/women-artificial-intelligence-mitigating-gender-bias.

Grewal, K. K. (2015). International Criminal Law as a Site for Enhancing Women's Rights? Challenges, Possibilities, Strategies. *Feminist Legal Studies*, *23*(2), 149–165.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175.

Hudson, N. F. (2010). *Gender, human security and the United Nations: Security language as a political framework for women*. *Routledge critical security studies*. Routledge.

Human Rights Watch. (2020). *Saudi Arabia: End Male Guardianship*. Retrieved April 30, 2020, from https://www.hrw.org/endmaleguardianship.

IPU (Ed.). (2020). *Women in Politics: 2020*. Retrieved July 1, 2020, from https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjvqYi5pqzqAhUD0qYKHcAaAB4QFjAAegQIARAB&url=https%3A%2F%2Fwww.ipu.org%2Ffile%2F8996%2Fdownload&usg=AOvVaw3D4HZ4FXk6E_YZJrnXSWQj.

Johnson-Freese, J. (2019). *Women, peace and security: An introduction*. Routledge Taylor & Francis Group.

Köver, C. (2019). *App Absher: Männer überwachen Frauen nicht nur in Saudi-Arabien.* Retrieved May 1, 2020, from https://netzpolitik.org/2019/app-absher-maenner-ueberwachen-frauen-nicht-nur-in-saudi-arabien/.

Krause, K., & Williams, M. C. (Eds.). (1997). *Borderlines: v.8. Critical Security Studies: Concepts and Cases*. Minneapolis. University of Minnesota Press.

Linaki, E. (2014). Cyber warfare and international humanitarian law: A matter of applicability. *Humanitäres Völkerrecht - Informationsschriften*, *27*(4), 169–176.

Locker, T., & Hoppenstedt, M. (2017). *Mehr als tausend Deutsche nutzen Spionage-App: "100 Prozent Erfolg - übermorgen ist meine Scheidung"*. Retrieved May 1, 2020, from https://www.vice.com/de/article/ezjdbj/mehr-als-tausend-deutsche-nutzen-spionage-app-100-prozent-erfolg-uebermorgen-ist-meine-scheidung.

Manjoo, R. (2014). *Submission from UN Special Rapporteur on Violence against Women: to the Open Working Group on post 2015 SDGs*. Retrieved June 19, 2020, from https://sustainabledevelopment.un.org/content/documents/3337RM%20submission%20to%20OWG%20on%20post%202015%20SDGs.pdf.

Matsubara, M. (2017). *Why Women in Cybersecurity Are Important, In Japan and Everywhere.* SecurityRoundtable.org, powered by Palo Alto Networks®. Retrieved April 28, 2020, from https://www.securityroundtable.org/women-cybersecurity-important-japan-everywhere/.

Mazurana, D., & McKay, S. (2001). Women, girls, and structural violence: A global analysis. In Christie, D. J., Wagner, R. V., & Winter, D. A. (Ed.), *Peace, conflict, and violence : peace psychology for the 21st century* (pp. 130–138). Prentice Hall.

Mills, E. (2010, December 1). *Demilitarizing Cybersecurity (Q&A)*. Retrieved June 22, 2020, from https://www.cnet.com/news/big-sale-in-ubisoft-town-save-up-to-80-on-games-sitewide/.

Molutsi, P. (2000). The interaction between state and civil society in southern Africa: Prospects for peace and security. In L. Wohlgemuth (Ed.), *Common security and civil society in Africa* (pp. 180–189). Nordic Institute of African Studies.

Morgan, S. (2019). *Women Represent 20 Percent Of The Global Cybersecurity Workforce In 2019.* Cybersecurity Ventures. Retrieved April 28, 2020, from https://cybersecurityventures.com/women-in-cybersecurity/.

NATO Review. (2017, August 3). *Women, Peace and Security: shifting from rhetoric to practice*. Retrieved May 4, 2020, from https://www.nato.int/docu/review/articles/2017/03/08/women-peace-and-security-shifting-from-rhetoric-to-practice/index.html.

O'Connell, M. E. (2008). Defining Armed Conflict. *Journal of Conflict and Security Law, 13*(3), 393–400.

Oxford University Press. (2014). *Oxford Online Dictionary: Cybersecurity*. Retrieved May 22, 2018, from https://www.lexico.com/definition/cybersecurity.

phoenix. (2019, January 8). *Pressekonferenz mit Bundesinnenminister Horst Seehofer zum "Datenklau-Skandal"*. Retrieved June 19, 2020, from https://www.youtube.com/watch?v=ownPbstZEKM.

Poster, W. R. (2018a). Cybersecurity needs women. *Nature*, *555*(7698), 577–580.

Poster, W. R. (2018b). Gender trouble in cyberwar: Multiple masculinities and femininities of a cyberspy in the War on Terror. In J. Hearn, E. Vasquez del Aguila, & M. Hughson (Eds.), *Routledge advances in feminist studies and intersectionality. Unsustainable institutions of men: Transnational dispersed centres, gender power, contradictions* (pp. 188–201). Routledge.

Reardon, B., & Hans, A. (Eds.). (2019). *The gender imperative: Human security vs state security* (Second edition). Routledge.

Reeves, A. (2012). Feminist Knowledge and Emerging Governmentality in UN Peacekeeping. *International Feminist Journal of Politics, 14*(3), 348–369.

Schmitt, M. N. (2011). Cyber operations and the Jus in Bello: Key issues. *Israel Yearbook on Human Rights, 41 (2011)*, 89–110.

Sharland, L., & Smith, H. (2019). Cyber, technology and gender: what are we missing? In L. Sharland & G. Feely (Eds.), *Strategic insights: Vol. 140. Women, peace and security:*

*Defending progress and responding to emerging challenges* (28-29). Australian Strategic Policy Institute.

Shepherd, L. (2008). *Gender, Violence and Security: Discourse as Practice* (1st ed.). Zed Books.

Shepherd, L. (2016). Making war safe for women? National Action Plans and the militarisation of the Women, Peace and Security agenda. *International Political Science Review*, *37*(3), 324–335.

Shepherd, L., & Kirby, P. (2016). The futures past of the Women, Peace and Security agenda. *International Affairs*, *92*(2), 373–392.

Sjoberg, L., & Via, S. (2010). *Gender, war, and militarism: Feminist perspectives*. *Praeger security international*. Praeger.

Syed, R., Khaver, A. A., & Yasin, M. (2019). *Cyber Security: Where Does Pakistan Stand?* Retrieved June 22, 2020, from http://hdl.handle.net/11540/9714.

Tamang, D. (2013). Gendering International Security. *International Studies*, *50*(3), 226–239.

Thompson, L. (2020, January 14). *Mexican Diplomacy Has Gone Feminist: Andrés Manuel López Obrador's administration has boldly reoriented its foreign policy toward gender equality.* Retrieved July 8, 2020, from https://foreignpolicy.com/2020/01/14/mexican-diplomacy-feminist-foreign-policy/.

Tickner, J. A. (1997). You Just Don't Understand: Troubled Engagements Between Feminists and IR Theorists. *International Studies Quarterly*, *41*(4), 611–632.

Tickner, J. A. (2006). Feminism meets International Relations: some methodological issues. In B. A. Ackerly, M. Stern, & J. True (Eds.), *Feminist Methodologies for International Relations* (pp. 19–41). Cambridge University Press. https://doi.org/10.1017/CBO9780511617690.003

True, J. (2005). Feminism. In S. Burchill (Ed.), *Theories of International Relations* (3rd ed., pp. 237–259). Palgrave Macmillan Ltd.

United Nations. Charter of the United Nations and Statute of the International Court of Justice. (1945). Retrieved April 30, 2020, from http://www.unwebsite.com/charter.

United Nations General Assembly. Countering the use of information and communications technologies for criminal purposes, https://undocs.org/en/A/RES/74/247 (2019). Retrieved July 5, 2020, from https://undocs.org/en/A/RES/74/247.

United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime: Draft - February 2013*. Retrieved July 5, 2020, from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

United Nations Security Council. UN Security Council Resolution 1820 (2019), Women and Peace and Security, S/RES/1820 (2008). Retrieved July 5, 2020, from http://unscr.com/en/resolutions/1820.

United Nations Security Council. UN Security Council Resolution 1889 (2009), Women and Peace and Security, S/RES/1889 (2009). Retrieved July 5, 2020, from http://unscr.com/en/resolutions/1889.

United Nations Security Council. UN Security Council Resolution 2493 (2019), Women and Peace and Security, S/RES/2493 (2019). Retrieved July 5, 2020, from http://unscr.com/en/resolutions/doc/2493.

United Nations Security Council. (2019). *Women and peace and security - Report of the Secretary-General*. Retrieved May 4, 2020, from https://www.peacewomen.org/sites/default/files/N1930837.pdf.

Vogelstein, R. B. (2019). *Five Questions on Feminist Foreign Policy: Margot Wallström*. Retrieved May 4, 2020, from https://www.cfr.org/blog/five-questions-feminist-foreign-policy-margot-wallstrom.

Walker, S. (2020). Cyber Dystopia. *The Ecosprinter*(1), 8–9. https://www.ecosprinter.eu/blog/cyber-dystopia/

Waltz, K. N. (2018). *Man, the state and war: A theoretical analysis* (Anniversary edition). Columbia University Press.

WILPF. (2015). *Transforming Violent Masculinities to Move the WPS Agenda Forward*. Retrieved May 15, 2020, from http://www.peacewomen.org/node/95466.

UN Women, & Coomaraswamy, R. (2015). *Preventing conflict, transforming justice, securing the peace: A global study on the implementation of United Nations Security Council resolution 1325*.

Women in CyberSecurity. (2019). *About WiCyS: How Companies Benefit from Engagement with WiCyS*. Retrieved April 28, 2020, from https://www.wicys.org/about-wicys.

The World Bank. (2018). *Population, female*. Retrieved April 28, 2020, from https://data.worldbank.org/indicator/SP.POP.TOTL.FE.IN.

World Economic Forum. (2019, March 5). *5 charts that reveal the state of the global arms trade*. Retrieved June 3, 2020, from https://www.weforum.org/agenda/2019/03/5-charts-that-reveal-the-state-of-the-global-arms-trade/.

World Health Organization. (2013). *Global and regional estimates of violence against women:: prevalence and health effects of intimate partner violence and non-partner sexual violence*. Retrieved April 30, 2020, from https://apps.who.int/iris/bitstream/handle/10665/85239/9789241564625_eng.pdf;jsessionid=A7CFE302BC537ED45B917841BD3C9939?sequence=1.

Wright, H. (2015). Ending Sexual Violence and the War System – Or Militarizing Feminism? *International Feminist Journal of Politics*, *17*(3), 503–507.

Wright, H. (2019). "Masculinities perspectives": advancing a radical Women, Peace and Security agenda? *International Feminist Journal of Politics*, 1–23.

Zeit Online. (2019). *Massiver Datenklau: Hunderte Prominente sind Opfer*. Retrieved July 4, 2020, from https://www.zeit.de/news/2019-01/04/massiver-datenklau-hunderte-prominente-sind-opfer-190104-99-429921.

# 9. Declaration of Authorship

I hereby declare that I have written this work on my own and have not used sources and resources other than those I have indicated. The parts of the work taken from other works, literally or by analogy, have been identified in each individual case, indicating the sources (including the World Wide Web and other electronic text and data collections).

I further assure that the work in the same or similar version was not yet part of another examination. I am aware that any act of contravention must be considered an attempt to deceive, as a result of which the course is judged failed and the recognition of the written work as examination is excluded.

I am aware that the Department of Studies and Teaching of the University of Erfurt will be informed about any attempt to defraud and plagiarism will be judicially considered a criminal offense. I have taken note of the statements on the handling of attempts at deception on the homepage of the University of Erfurt.
(http://sulwww.uni-erfurt.de/pruefungsangelegenheiten/taeuschung/taeuschen.asp)

Erfurt, 14.07.2019 ……..……

Clara Winkler