Swedish Defence University

Important system updates needed! Masculinised logics and gendered path dependence in the European Union's cybercrime institutions

Felicia Rhedin

Thesis, 30 ECTS (hp)
Political Science with a focus on Crisis Management and Security
Master's Programme in Politics and War
Autumn 2019
Supervisor: Sara Bondesson
Word count: 14222

Abstract

This thesis approaches the EU's cybersecurity discourse from a feminist angle, using a theoretical perspective based on feminist institutionalism and path dependence. The aim is to explore what conceptual logics make it possible for the EU to conceptualise cybersecurity and -crime "problems" in a genderblind way. Making use of Carol Bacchi's post-structural policy analysis "What is the Problem Represented to Be?" I conduct an analysis of the EU's cybercrime institutions, focusing on the main EU cybercrime organisation – the EC3. Through analyses of relevant EU and EC3 texts, I find that the EU's cybercrime institutions are marked by a masculinised way of thinking about cybersecurity and -crime issues, mainly derived from traditional security discourse, which has created path dependence for how cybersecurity and -crime can be understood. Four logics are identified: the control of cyberspace logic which positions cyberspace as the referent object of security; a technical logic which proposes that the risks faced by individuals and societies can be mitigated by increasing the security of ICT products, processes and services; the vulnerability of children logic which constructs children as a vulnerable group whose victimisation is morally necessary to counter; and the end-user responsibility logic which assumes that some forms of issues are best countered by changing the behaviour of the victims. These logics in different ways make the incorporation of a gender perspective more difficult.

Keywords: Cybersecurity, cybercrime, European Union, EU, EC3, feminist institutionalism, path dependence, cyber violence, VAW, VAWG

Table of content

1. Introduction

When composer John Cage wrote some of his most notable musical works, he systematised chance as a tool for composing. He realised that whatever he could create from his own mind would always be confined to what he already knew. Only by leaving the pitches, durations and dynamics of the sounds to chance would the piece be free from the composer's subjectivity and limited understanding of what music can be (Le Bail, 2018). This anecdote might seem random in a thesis on the European Union's (EU) cybersecurity institutions, but I choose to lead with it because it points to the core of its subject – how actors are constrained by the norms and values that shape how they perceive the world.

There is no one commonly accepted definition of cybersecurity, but generally it can be understood as "the set of protocols, technologies, and practices designed to protect against threats mediated by digital technology." (Slupska, 2019, p. 84). The definition of cybersecurity is, however, highly contested and framing it in any given way will have consequences in terms of what policy and strategy options are rendered thinkable.

In 1996 the EU adopted gender mainstreaming as a tool for ensuring gender sensitivity in all policy and institutional development (European Commission, 1996). A sizable body of feminist literature has, however, argued that implementation has been lacking (Bretherton, 2001; Cavaghan, 2017; Stratigaki, 2005; True, 2003; Walby, 2005). The area of cybersecurity, and more specifically – cybercrime, is particularly interesting from a feminist perspective because of the highly gendered issues which could fall into this category, including for example cyber stalking, electronically enabled trafficking, non-consensual pornography and hate speech against women (Eaton, Jacobs & Ruvalcaba, 2017; Pew Research Center, 2014). There are reasons to expect the EU to acknowledge gendered technology-facilitated violence in cybersecurity and -crime policies. The European Commission has recognised violence against women (VAW) as a human rights violation, and cyber violence as a form of VAW (European Commission, n.d.). Article 83 in the Treaty of the Functioning of the European Union makes it possible to initiate judicial cooperation in criminal matters and to establish minimum rules in regard to definitions of criminal offences and sanctions in the areas of computer crime and serious crime with a cross-border dimension (Van Der Wilk, 2018). Furthermore, the Commission communication establishing the European cybercrime centre (EC3) formulates three strands of cybercrime for the centre to focus on, one of which is "[c]ybercrimes which cause *serious harm to their victims*, such as online child sexual exploitation" (European Commission, 2012, p. 4, emphasis added). Indeed, cyber violence and other forms of online perpetrations committed against women have been shown to have severe impact on their victims. Victims of online harassment and abuse have for example reported experiences of stress, anxiety and fear for their physical safety as a result from their online experiences (Amnesty International, 2017).

As feminist scholars have pointed out, the mainstreaming of gendered security issues is achieved only when "gender issues are given substantive meaning in specific social contexts and policymaking processes" (True, 2003, p. 376). Thus, a full integration of a gender perspective into the EU's cybersecurity and -crime policies should include acknowledging gendered security issues, introducing efforts to increase knowledge about their nature and extent and proposing specific political actions counter them. Surprisingly, gender is virtually absent from the examined EU policies on cybersecurity and cybercrime. Gender is explicitly mentioned only when referring to gender balance on boards and working groups and as feminist scholars have demonstrated, increasing the sheer number of women in political units is insufficient for achieving gender-sensitive policy (Kronsell & Magnusdottir, 2015). Because gender is virtually absent from the EU's cybersecurity and -crime policies, this thesis takes on the analytical task to explore what conceptual logics make it possible for the EU to conceive of cybersecurity and -crime "problems" in a genderblind way. This is explored using a theoretical perspective based on feminist intuitionalism and path dependence, which "highlights the durability in the dynamics of gender relations" (Kronsell, 2016, p. 311). Feminist institutionalism would suggest that the absence of gender can be understood in relation to the deeply institutionalised masculine logics in security and technology institutions.

The technological sector, including the emerging field of cybersecurity, is persistently dominated by male bodies (EIGE, 2018; Peacock and Irons, 2017). Earlier research has identified technology as a masculine field and a domain of masculine power (Cockburn, 1985). Previous research has also found a prevalence of historical gender norms and masculine logics in other security domains, including the EU's military institutions (Kronsell, 2016; Ericson, 2018a). The traditional security discourse centres around a relationship of protection – in which the protector is elevated to a position of incontestable, superior authority and the protected is expected to be submissive and grateful (Tickner, 1991; Young, 2003). As feminist scholars have stressed, the protector-protected roles are gendered, as protection is associated with masculinity and being in need of protection is associated with femininity. The gendered logic of this relationship is essential. Because assuming the role of protector is historically and socially rooted as the ultimate form of chivalry and masculinity it serves to justify notions of security. It also reinforces a hierarchical structure between masculinities and femininities, giving primacy to a Western, masculine identity construction. Finally, the experiences of women go way by due to a neglection of gendered security issues and a simplified image of women (Ericson 2018b; Hutchings, 2008; Tickner, 2002; Stiehm, 1982). Thereby, the traditional security discourse has been criticised for ignoring the violence that usually occurs in the "private" sphere of the household or family (Blanchard, 2014). Applying a feminist perspective is thus helpful for understanding gendered power inequalities in political and public life (Mackay, Kenney & Chappell, 2010).

The connection between security and masculinity is particularly interesting for the case of EU's cybersecurity and -crime institutions because recent scholarship has demonstrated that a collective securitisation of cyberspace has been visible in the EU (Christou, 2019). Securitisation commonly refers to "a concept that addresses specific elements of how power asymmetries gain legitimacy in neoliberal forms of governance, fostering a 'political culture of danger'" (Ericson, 2018b, p. 96). It can generally be understood as a discursive process of presenting an issue as a substantial threat that warrants taking extraordinary measures, thereby moving the issue from the political realm into the realm of security (Buzan, 1991; Kasper, 2014). Following a series of impactful events and threat trends, EU institutional actors have carried out securitising moves, which have been accepted by the member states through the adoption of new legal frameworks, instruments and mechanisms. The EU has increasingly established itself as a cybersecurity actor, albeit complex and asymmetric across the three different cybersecurity pillars – cybercrime, network and information security and cyber-defence (Christou, 2019; see also Carrapico & Barrinha, 2017). As the field of cybersecurity is growing, recent feminist scholarship has flagged the risk of reproducing masculinist dynamics within it (Slupska, 2019). Although the body of research on cybersecurity is growing, the EU's cybersecurity institutions have thus far not been approached from a feminist perspective.

1.1. Aim and research problem

The aim of this thesis is to explore what conceptual logics make it possible for the EU to conceptualise cybersecurity and -crime "problems" in a genderblind way, despite women being disproportionally subjected to certain forms of technology-facilitated violence.

Applying a theoretical perspective based on feminist intuitionalism and path dependence, I will explore and critically reflect on this using a slightly revised version of Carol Bacchi's (2009) post-structural policy analysis "What is the problem represented to be?", utilising the following analytical question:

1. *What is the problem represented to be?*
2. *What deep-seated conceptual logics underlie this representation of the "problem"?*
3. *What is left unproblematic in this problem representation? Where are the silences? Can the "problem" be conceptualised differently?*
4. *What effects are produced by this representation of the "problem"?*

These questions will be applied in an analysis of the EU's cybersecurity and -crime institutions, examining the EU's Cybersecurity Strategy and Cybersecurity Act as well as a range of material relating to the EU's cybercrime centre (Europol's EC3), which is the main organisation under study. To achieve the aim of this thesis I will take help of previous research, particularly feminist research on the subjects of gender, security and technology. The analysis will also make use of the concept "referent object of security", derived from the Copenhagen School. The referent object of security refers to the object which is considered to be under threat, and which must be protected. In other words, the referent object of security is the object for whom security is for (Buzan, 1991).

In addition to the aim of this thesis, a final contribution will be to make suggestions on how a gender-sensitive conceptualisation of cybersecurity and -crime "problems" could be conceived.

1.2. Research question

- What conceptual logics make it possible for the EU to conceptualise cybersecurity and -crime "problems" in a genderblind way?

2. Previous research

2.1. The social construction of cyberspace

The virtual nature of cyberspace makes it especially challenging to reach a common conceptualisation of what it is (Kasper, 2014). Drawing from securitisation theory, Myriam Dunn Cavelty (2012; 2013) examines the social construction of cybersecurity in the United States (US). Although the perception of cybersecurity as an uncontested domain of national security dominates the modern cybersecurity discourse, she finds competing "threat representations" – ways to depict what counts as a risk or threat – among different communities of actors within this discourse. These threat representations each build on different conceptualisations of what cyberspace is and, perhaps more importantly, come with different social and political effects. As Dunn Cavelty puts it "[t]he way cyberspace is imagined and defined has consequences for the way any type of action or strategy is conceptualized" (Dunn Cavelty, 2013, p. 108). By conceptualising what cyberspace is and what threats exist within it in any given way we delimit the range of policy options available to us.

Turning the gaze towards the international realm, there are particular ways in which threat perceptions manifest themselves in liberal democracies. While the principal aim of cybersecurity in liberal, democratic countries is to protect information networks and databases as well as ensure the functioning of the global economy, military and intelligence institutions – for various historical and institutional reasons – hold dominant roles in cybersecurity. Military and intelligence agencies are institutions which are tasked with the protection of national security, not free and open networks. Thus, we can expect a conflict over which referent object of security should be emphasised. For example, many government agencies stockpile computer software vulnerabilities to use as prospective "weapons" of cyber espionage or warfare, by which the security of the "own country's networks" trumps the integrity of networks abroad (Deibert, 2018). An illustrative example of how such policies can pan out is the 2017 WannaCry ransomware attack, where the antagonists appear to have utilised an exploit stolen from and developed by the US National Security Agency (NSA) (The WannaCry ransomware attack, 2017). National security can also take precedence over the referent object of the individual user (Deibert, 2018), as in the case of the NSA surveillance campaign. Leaked documents revealed that nearly 60 million communication connections had been under surveillance, affecting both US and foreign citizens. The goal of the extensive surveillance was to prevent terrorist activity (Trifonov, 2017). The tension between different referent objects is also visible in the case of the EU's 2006 data retention directive. The directive obliged electronic communication and network providers to retain data generated or processed by the provider, including users' traffic and location data as well as the data necessary to identify the user (CCDCOE, n.d.). In 2014 the European Court of Justice declared the directive invalid on the ground that it exceeded the limits of proportionality. In particular, the Court held that the directive seriously infringed on the right to privacy and the right of personal data protection of individuals ensured by the Charter of Fundamental Rights (Papademetriou, 2014).

A somewhat competing view is that the cybersecurity sector, although marked by multiple different discourses, possesses a significant degree of coherence because it ties contesting referent objects of security together. In particular, the security of networks has implications beyond the network itself. The break-down of a network can have consequences for other referent objects – individuals, collectives, economies and states – which is what makes the security of networks a critical political issue (Hansen & Nissenbaum, 2005). Hansen and Nissenbaum do, however, acknowledge a central shortcoming in the conceptualisation of cybersecurity discourses as "constellations of connected referent objects", namely that it silences insecurities of marginalised groups. Examining only the dominant discourses will thereby omit insecurities which have not gained political recognition as security issues.

2.2. Securitisation, the construction of gender and the silence of women

Feminist theorists have argued that there is a link between securitisation and masculinity construction (Ericson, 2018b). In this line of theoretical reasoning, protection is understood as a form of power relationship in which the protector tries to "control the lives of those he protects – in order to 'better protect' them" (Stiehm, 1982, p. 372). The roles in this relationship are gendered, as providing protection is associated with masculinity and being in need of protection is associated with femininity (Tickner, 1992). The notion of security evokes a patriarchal logic in which a strong, masculine protector defends a vulnerable femininity, and the state is promoted as the primary provider of security. These dynamics are triggered, not only in wartime, but also in the face of other threats, such as crisis situations, terror attacks and hazards (Ericson, 2018b). Often, women and children are discursively positioned under the umbrella of protected, vulnerable femininities, but this is also the case for men who do not conform to the masculine ideals – a notion commonly referred to as "hegemonic masculinity". Seema Narain, building on the theoretical contributions of Ann Tickner, describes hegemonic masculinity as defining "what masculine men should be, in opposition to femininities, which are less valued." (2014, p. 180).

In her critique of the US's security regime after September 11 Iris Young formulates a theory of masculinist protectionism, building on Foucault's notion of pastoral power. Rather than a relationship of repressive domination, this "authoritarian security paradigm" takes the form of a patriarchal household. The masculine protector's authority comes, not from acts of repression, but from his willingness to sacrifice and take risks for the sake of others. The feminine subordinate does not resist or even resent the protector's dominant position but admires his courage and accepts his guardianship (Young, 2003). She might consider her role rather comfortable, since she is not required to get her hands dirty with warfare (Stiehm, 1982).

However, she is also expected to be submissive and to abstain from political decision-making (Kronsell, 2016). As Young puts it:

> The logic of masculinist protection works to elevate the protector to a position of superior authority and to demote the rest of us to a position of grateful dependency. Ideals of democratic equality and accountability go by the wayside in the process. (Young, 2003, p. 13).

The protector logic has both an inward and an outward dimension. Inwards, the logic takes the form of a guardianship. Facing outwards, the protector defends against an outside enemy. Thus, two types of vulnerable femininities can be expected: a feminine "other" to save and a homeland femininity to defend (Young, 2003; 2007). Looking at the EU, earlier research has identified these dynamics in the Union's Common Security and Defence Policy (CSDP) and military institutions. The EU protector masculinity aims to defend the femininities both at home and in outside conflict areas but does so by engaging in teaching and training rather than military interventions. In this way, the EU military masculinity logic works in a different – and arguably more benign – way than for example the US's (Kronsell, 2016). The US masculinity uses the freeing of subjugated women as justification for going to war. But such actions rarely end up changing patriarchal structures long-term, and the women who were meant to be "saved" instead find themselves exposed to the horrors of warfare (Khalili, 2011; Masters, 2009; Tickner, 2002; Young, 2003). Although perhaps less harmful, the EU military protector logic nevertheless constructs femininities without agency. The EU femininities are passive and silent subjects under the rule of a masculine defender (Kronsell, 2016).

For the protection of femininities to be valid, another masculinity must also be constructed – a masculine "other". The masculine other has not only failed to protect the feminine other but is assumed to be responsible for the abuse she has suffered. These "bad" men must either be defeated or taught to do better by the "good" men (Kronsell, 2016). As Ericson argues, the notion of "good" and "bad" men rests on racist agendas as it constructs white men as the "good" men who protect women from "bad", "foreign" men (Ericson, 2018b).

2.3. Cybersecurity and gender

2.3.1. Gendered cybersecurity issues

Research on cybersecurity and gender is – at best – scarce. There are studies indicating that women are more likely than men to be victims of certain forms of cyber violence, such as cyber stalking, non-consensual pornography (the sharing of intimate images of another person without their consent) and online sexual harassment (Pew Research Center, 2014; Eaton, Jacobs & Ruvalcaba, 2017). Furthermore, women are likely to experience greater levels of emotional distress as a result of their victimisation (Staude-Müller, Hansen, & Voss, 2012). However, data on the subject is still lacking (EIGE, 2017). In 2017 the European Commission issued a special Eurobarometer surveying Europeans' attitude towards cybersecurity. Participants were asked about their experience of various cybercrimes, such as identity theft, scam emails and malware. Crimes which tend to mainly affect women, for example online sexual harassment and non-consensual pornography, were not included in the survey (European Commission, 2017). This exclusion of gendered security issues is illustrative of a knowledge gap on how violence against women is facilitated by technology.

A 2015 study by the European Union Agency for Fundamental Rights (FRA) on violence against women in the EU indicates a correlation between internet use and the prevalence of cyber harassment. Cyber harassment was significantly more common in countries with high rates of internet access and less so in countries with low levels of internet access. Experiences of cyber harassment were also more common in younger age groups, which could partially be explained by the more widespread use of internet in the younger population. These findings are particularly relevant given the current rapid expansion in access to new technologies. As more and more people get access to internet and start using new technologies the occurrence of cyber harassment and other technology-facilitated forms of abuse risks increasing (FRA, pp. 104-5).

Antifeminist movements have also taken advantage of the opportunities provided by the expansion of the internet. Online platforms are used to form social networks to share antifeminist ideas and recruit new members and online-facilitated strategies are employed to threaten and harass feminist groups and individuals. For example, doxing (revealing personally identifiably information online), cyber stalking, online death threats and other forms of public shaming are popular tools in antifeminist circles (Holm, 2019, p. 140). A 2017 survey commissioned by Amnesty International highlights the impacts of online abuse and harassment on women's lives. 41% of the surveyed women who had experienced online abuse or harassment stated that they had on at least one occasion feared for their physical safety as a result of their online experiences. A majority of the respondents with experiences of online abuse or harassment also reported having suffered from psychological effects such as stress, anxiety or panic attacks. Furthermore, online abuse and harassment of women can result in self-censorship and exclusion. 76% of the women who reported that they had experienced abuse or harassment on a social media platform said that they had made changes to the ways in which they use the platforms. A third even stated that they had refrained from sharing content that expressed their opinions on certain issues online (Amnesty International, 2017).

Earlier research suggests a co-occurrence between online and offline violence, meaning that cyber violence and hate speech online should be understood as existing on the continuum of violence against women and girls (VAWG), rather than as isolated phenomena (Leemis et al., 2019; McGlynn Rackley & Houghton, 2017). As Lumsden and Morgan put it, new forms of media can "exacerbate issues surrounding sexual violence through the creation of digital spaces in which the perpetration and legitimisation of sexual violence takes on new qualities." (Lumsden & Morgan, 2017, p. 928). As such, online perpetrations can be understood as part of a larger context of violence against women and girls.

2.3.2. Masculinity and masculine bias in cybersecurity

Julia Slupska's (2019) study of so-called smart home technology provides an initial feminist critique of cybersecurity research and technology design. The study uncovers a tendency for smart home threat analyses to ignore gendered technology-facilitated security issues like non-consensual pornography and intimate partner violence. Although women run a considerable risk of being subjected to violence or abuse from a trusted "insider", such as a current or former partner, security analyses of smart home devices fail to account for threats coming from the inside of the home. Instead, threat analyses tend to focus on a possible outside adversary attempting to breach the home's security barriers. These finding are consistent with feminist international relations (IR) critique against the private/public binary, in which the private home is imagined as a safe place which should be shielded from political scrutiny. Such a binary understanding leads to the neglect of gendered security issues taking place in the "private sphere", like intimate partner violence, and removes them from the public and political agenda. Slupska argues that by overlooking gendered technology-facilitated security issues, the emerging field of cybersecurity risks reproducing these dynamics.

Slupska's study also highlights another important aspect of cybersecurity – that it matters who is involved in technology design. When only a narrow, homogenous part of society develops a technology, their biases and values will be reflected in the end product. Sandra Harding's (1991) feminist standpoint theory emphasises the social situation of the epistemic agent in the production of knowledge. Knowledge produced without considerations for the particular issues faced by marginalised groups risks ending up with a Western, androcentric bias. Harding therefore argues that research must start thinking from (all) women's lives, not just the lives of the dominant groups, and that marginalised groups are particularly well-positioned to do so (Harding, 1991). Still, science, technology, engineering and mathematics (STEM) professions are persistently dominated by men, with women constituting only around 33% of graduates in STEM tertiary education and 13% of graduates in STEM vocational education in the EU (EIGE, 2018). Furthermore, women account for a mere 11% of the cybersecurity workforce globally. In Europe, this figure is as low as 7%, according to a study cited by Peacock and Irons (2017). The dominance of men in cyber professions is indeed worth mentioning as "[i]nstitutions largely governed by men have produced and recreated norms and practices associated with masculinity and heterosexuality" (Kronsell, 2005, p. 281).

There is also a power dimension to the masculine overtone in technology. In Cynthia Cockburn's 1985 *The Machinery of Dominance: Women, Men, and Technical Know-How* an interlinkage between masculinity, technology and gendered distribution of power is observed. She demonstrates how promises of gender neutrality in new technologies have quickly been shattered through gender segregation of work, to the advantage of men (Cockburn, 1985). Historically, women have often been involved in the early stages of new technology fields, such as computing. But as the field has become successful, men have assumed dominance in the more technically advanced tasks associated with it and women have been removed from decision-making positions (Shortt, 1998). The result is that the technological domain is (re)constructed as gendered. Furthermore, segregation of the labour market, associating low-skill, low-paid roles with female workers and high-skill, high-paid roles with male, means that gender inequality is reproduced (Cockburn, 1985). More recent studies suggest that the intimate connection between technology and masculinity has been difficult to break from (Mellström & Holdt, 2011).

What can be generally concluded from this literature review is that there is a lack of feminist perspectives in cybersecurity research. While there is some research highlighting the absence of gender perspectives in cybersecurity and technology, and the relevance of such considerations, no studies have been conducted which investigate the discursive hindrances to the incorporation of gender-sensitive conceptualisations in the cyber domain. This thesis also attempts to contribute to feminist IR scholarship by approaching an emerging security domain using feminist theory.

3. Theory

3.1. Understanding gender

For the past decades, feminist perspectives have provided a critical lens to the previously gender-blind field of IR and security studies (Ackerly, Stern, & True, 2006). Most contemporary feminist theory rejects the positivist claim that the world is directly accessible to the researcher. Instead, knowledge is seen as socially constructed, which is why claims about objectivity and the neutrality of language must always be questioned (Tickner, 1992, p. 36).

This thesis understands gender as "a constitutive element of social relations based upon perceived (socially constructed and culturally variable) differences between women and men, and as a primary way of signifying (and naturalizing) relationships of power and hierarchy" (Mackay, Kenny & Chappell 2010, p. 580). As such, the element of gender operates not only at the interpersonal level – how humans identify themselves and organise themselves in relation to others – but on an institutional level as well. It follows that this line of feminist scholarship does not attempt to add "gender" as a category of analysis, but rather to lay bare the way in which existing logics are already gendered (Masters, 2009). As Young puts it:

> Viewing issues of war and security through a gender lens, I suggest, means seeing how a certain logic of gendered meanings and images helps organize the way people interpret events and circumstances, along with the positions and possibilities for action within them, and sometimes provides some rationale for action. (Young, 2003, p. 2).

Older feminist scholarship has been criticised for concentrating solely on the connection between masculinity and security, thereby reproducing a simplified image of women as peaceful and omitting women's experiences (Sylvester, 2013, p. 39). Contemporary scholars have therefore argued for the importance of also understanding the femininities at play (Khaili, 2011; Blanchard, 2014). Attempting to contribute to the larger field of feminist IR and security studies, this thesis applies a theoretical perspective based on feminist institutionalism and path dependence, adopted from Kronsell (2016).

3.2. Feminist institutionalism

Feminist institutional theory (FI) has its roots in feminist political science and new institutionalism. While historically, the formal inclusion of women in decision-making has been highlighted as essential (a concept often referred to as "critical mass"), growing evidence suggests that increasing the sheer number of women is insufficient for generating gender-sensitive policy (Kronsell & Magnusdottir, 2015; Shirin & Waylen, 2008). FI understands this as an issue of institutionalised norms which shape the perceptions and behaviours of policymakers.

> The rules of the game – be they relating to legislatures, courts, bureaucracies or federal structures – can be seen as gendered as they prescribe (as well as proscribe) 'acceptable' masculine and feminine forms of behaviour, rules and values for men and women within institutions. (Mackay et al., 2010, pp. 581-582).

FI, building on new institutionalist theory, understands institutions as "sets of rules" that guide the behaviour of actors. Institutions are not equated with political organisations. Rather, organisations, like individuals, are seen as players in a game for which institutions set the rules. Institutions thus exist within, between, above and around organisations. This is not to say that organisations are irrelevant for institutional analyses. On the contrary, organisations are of high significance for two reasons – they are both constrained and enabled by existing institutional rules, and they work as arenas for the production of institutional rules. For FI both formal and informal institutions are considered important. Formal institutions are written down rules and violations of them are legally sanctioned, while informal rules are unofficial but generally accepted norms of which violations are socially sanctioned (Lowndes, 2010).

Situating themselves in the structure-agency debate, FI sees actors as having agency but being bounded by various institutional constraints. As Lowndes (2010) argues, actors are both products and producers of history. FI studies are particularly interested in the changes and continuities of institutions. Both change and stability are seen to be driven by (gendered) processes internal as well as external to the institutions. Endogenous sources of transformation and stability include dynamics of power and resistance within institutions. As a branch of feminist scholarship, there also is an innate transformative agenda to FI studies. By studying possibilities for institutional change, FI scholars aim to understand how transformation can come about (Mackay et al., 2010).

3.3. Path dependence

Path dependence suggests that institutions provide constraints that render certain courses of actions more or less appropriate. As used in FI, path dependence highlights how institutions tend to lock into place gendered norms of behaviour. These norms become embedded in the institutions, which could explain the persistence of historic gender norms. Even if formal barriers of entry for women have been removed, norms around gender that are entrenched in the organisation can nevertheless present challenges for women's inclusion and performance (Kronsell, 2016).

The prevalence of masculinised logics within other security domains (Kronsell, 2016; Ericson, 2018a; 2018b) as well as the dominance of male bodies and masculine biases in technology (Cockburn, 1985; EIGE, 2018; Peacock & Irons, 2017) would suggest path dependence also within the EU's cybersecurity institutions. FI would suggest that historical institutional rules have been inherited and translated into the new domain of cybersecurity – that the masculinist logics that have dominated the security discourse and the field of technology has created path dependence for how the emerging field of cybersecurity can be understood. Historical institutionalism argues that even informal institutional rules become difficult to break from and doing so will be sanctioned by social disapproval. In other words, we can suspect an institutionalisation of masculinised logics of security and technology, meaning that a new way of understanding cyberspace might not be easily accepted.

4. Methodology

The EU's cybersecurity architecture consists of three pillars: cybercrime, network and information security and cyber-defence and the respective responsibilities for these pillars are placed within different EU bodies. Out of the three pillars cyber-defence is the least developed due to its strong position as a national competence (Carrapico & Barrinha, 2017; Christou, 2019). Because of the complex and fragmented nature of the EU as a cybersecurity actor, a full analysis of the EU's three cybersecurity pillars would be beyond the scope of this thesis. As previously stated, the analysis will consist of an overview of the EU's cybersecurity institutions and a deeper analysis of the EU's cybercrime institutions, focusing on the EU's cybercrime centre EC3. Cybercrime, as defined in the EU's Cybersecurity Strategy refers to:

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

Cybercrime is one of the three priorities in the European Agenda for Security. Because of its cross-border dimension the EU is considered to be able to make a substantial difference in the area (European Commission, 2015). The European cybercrime centre EC3 was established in 2013, with the purpose to "act as the focal point in the fight against cybercrime in the EU" (European Commission, 2013b, p. 3). It was decided that the EC3 would be located in the EU's law enforcement agency (Europol) and focus on three areas:

> (i) Cybercrimes committed by organised crime groups, particularly those generating large criminal profits such as online fraud;
>
> (ii) Cybercrimes which cause serious harm to their victims, such as online child sexual exploitation; and
>
> (iii) Cybercrimes (including cyber-attacks) affecting critical infrastructure and information systems in the Union. (European Commission, 2013b, p. 4).

Because the topic of this thesis is clearly described and relatively bounded (the gender blindness in the EU's cybersecurity and -crime institutions) a post-structural single case study approach is deemed suitable. As Mohammed et al. argue (2015, p. 103), the case study is a useful methodological approach for post-structural researchers interested in exploring the discursive contexts that shape the phenomenon of interest. As such, this thesis does not make any claims to *explain* the observed phenomenon, but rather to uncover "conditions of possibility" that has allowed certain understandings to emerge, and others to be supressed. A post-structural case study "allows for the exploration of a deeper understanding of the broader discourses that shape a phenomenon, as well as how power/knowledge relations shape the behaviours and perceptions of people" (Mohammed et al., 2015, p. 97).

One of the most apparent methodological concerns in this thesis is that of confirmation bias, meaning that there is a risk that the data is interpreted in a way that supports the researcher's hypothesis. Subscribing to a post-structural research tradition, I recognise that complete objectivity cannot be achieved. Still, the analysis has been guided by the principal of confirmability, meaning that the researcher's values or theoretical inclinations should not be allowed to substantively intrude in the investigation (Bryman, 2012, p. 392-393). Bacchi (2009) also encourages researchers to subject their own interpretations to the same scrutiny as they do to the examined data. Bearing this in mind, my findings from the analysis have continually been questioned and re-evaluated throughout the process. I have also attempted to conduct and present my analysis in a transparent way.

It is important to note that this thesis attempts an in-depth exploration of an observed phenomenon and does not have the ambition to generalise or contribute to theoretical refinement. This, however, does not mean that the findings from this study could not be of relevance also to other contexts or situations.

4.1. Post-structural policy analysis: analytical framework

The methodological approach chosen for this thesis is Carol Bacchi's post-structural "What is the problem represented to be?" (WPR). WPR is a tool for analysing underlying assumptions in policies. It is based on the premise that policies and suggested solutions are not responses to real world "problems" that lie outside the policy process. Rather, "problems" are endogenous to policy. In the process of making policy to "solve" a "problem", the "problem" is given shape. WPR analysts make the case that governments hold an especially privileged position because their assumptions underpin the problem representations constituted in legislation and other instruments used to govern, meaning that their understandings of problems "stick" (Bacchi, 2009). This view is shared by FI theorists, who emphasise the way in which policy-making institutions (re)produce the gender norms within them through the production of policy, legislation and rulings (Mackay, et al., 2010). The importance of governments can also be said to be true in the case of the EU – a regional actor with legislative powers.

Because this thesis aims to explore what conceptual logics make it possible for the EU to conceptualise cybersecurity and -crime "problems" in a genderblind way, an approach which seeks to bring the implicit into the open is deemed particularly suitable. By critically examining the EU's problematisations of cybersecurity issues it will be possible to reveal something about what underpins the EU's genderblind representations of cybersecurity and -crime "problems". The method has also been chosen for its compatibility with the chosen theory. Like FI, WPR is concerned with both formal and informal rules – the legislature which make certain problem representations "stick" and the underlying, conceptual logics that make such understandings of the "problem" possible (Bacchi, 2009). Furthermore, it is of interest to FI studies, not only to understand the reproduction of gendered power distribution within institutions, but to uncover how these institutions can be transformed (Mackay et al., 2010). The WPR approach, incorporating a Foucauldian concept of power, has an inherent transformative agenda and invites the analyst to considered alternative ways to conceive of the "problem". WPR, in making visible the perspectives and issues silenced in any given policy, is thus a fruitful approach for feminist research concerned with the distribution of power.

The WPR approach contains a set of questions to guide the analysis and critically interrogate the chosen texts. This thesis will apply a slightly revised version of Bacchi's analytical WPR chart, adapted from Bacchi and Goodwin (2016, p. 20) and the following section will present the questions used for the analyses.

Question 1: What is the problem represented to be?

Question 1 is posed in order to clarify the implicit problem representations of the given policy. The argument is that because how we feel and think about something determines what we propose should be done about it, it is possible to reveal how an issue is thought about by looking at the proposed solution to it. The WPR approach recognises that contesting problem representations can exist simultaneously in the same texts and the analyst is encouraged to acknowledge such frictions, should they appear.

Question 2: What deep-seated conceptual logics underlie this representation of the "problem"?

Question 2 asks what underlying assumptions underpin the identified problem representations. Building on Foucault's notion of epistême, we ask what underlying "knowledge" about the world that has made it possible to conceive of the "problem" in the identified way. To help investigating deep-seated presuppositions, the chosen texts are examined for the operation of binaries (e.g. "private-public"), key concepts (e.g. "cybersecurity") and categories (in particular categories of people). These assumptions serve to delimit how an issue can be understood and by extension the policy solutions proposed (Bacchi, 2009).

Question 3: What is left unproblematic in this problem representation? Where are the silences? Can the "problem" be conceptualised differently?

Question 3 opens up for reflection on issues and perspectives that have not been considered in the identified problem representations. Here, the limitations and shortcomings of representations can be critically examined, by for example problematising simplified binaries and concepts found in the analysis performed in question two. With this question we are invited to consider what is silenced in the given representations of the problem (Bacchi, 2009).

Question 4: What effects are produced by this representation of the "problem"?

Question 4 helps us identify and assess the effects produced by particular problem representations. This does not entail measuring outcomes but rather reflecting critically on how the representations might affect different groups of people in uneven ways (Bacchi, 2009). Three different, but interconnective, types of effects can be considered: subjectification effects, discursive effects and lived effects. *Subjectification effects* refers to the kind of subjects the identified problem representations produce. To study *discursive effects* is to examine the ways in which specific problem representations set limits to what can be thought. Lastly, analysing *lived effects* means drawing attention to what impacts the subjectification and discursive effects has on the people's lives (Bacchi & Goodwin, 2016).

4.2. Material

As Bacchi (2009) argues, choosing texts for an analysis is in itself an interpretive process. Which texts I choose for my analysis will inevitably reflect my research interest. However, to minimise bias in the analysis, the principal of considering all the relevant data, even if it contradicts the given theory has been followed, as suggested by Harder (2010).

The first text chosen for the overview analysis is the 2013 *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, which outlines the EU's visions for the domain of cybersecurity, sets out roles and responsibilities for the relevant bodies and articulates the actions required for achieving the outlined vision. The second text is the *EU Regulation 2019/881*, commonly referred to as the Cybersecurity Act, adopted in April 2019. The Cybersecurity Act was developed as a response to EU-wide cybersecurity challenges and includes actions such as a renewed and permanent mandate for the EU's cybersecurity agency ENISA and the introduction of a European certification framework for ICT products, processes and services (European Commission, 2019).

In regard to cybercrime-specific texts, official documents relating to the EC3 have been used. These include documents outlining the tasks of the centre, such as a performance report, Europol's *EU Serious and Organised Crime Threat Assessment* (SOCTA) reports and *Internet Facilitated Crime Threat Assessment* (IOCTA) reports. The SOCTA report is published every four years and outlines the identified threat trends in the area of serious and organised crime in the EU, including cybercrime. The SOCTA serves as a key document in informing the EU Policy Cycle for Serious and Organised Crime in the EU, which determines the crime priorities for the upcoming four-year policy cycle (Council of the European Union, 2018). The IOCTA report is a yearly publication in which the Europol and the EC3 provide an overview of identified current and future cybercrime threats and trends, with a focus on the crime priorities set by the current Policy Cycle (Europol, 2017a). Lastly, some material such as webpages, campaign material and newsletters have been consulted. Such material is "highly relevant because it refers to stereotypes and binaries more clearly than official documents" (Kronsell, 2016, p. 314).

5. Analysis

5.1. What is the problem represented to be?

The non-human referent object problematisation

The first problem representation marking the cybersecurity documents is one I would call the *non-human referent object* problematisation. There is a tendency in the cybersecurity policies to focus on the security of cyberspace as a domain, and of objects such as networks, information systems and information and communication technology (ICT) products. The proposed solutions include technical solutions, such as efforts to enhance the security of ICT products, promote the adoption of network and information security standards and develop digital forensic tools and technologies for combating cybercrime, as well as suggestions for increased coordination among EU member states and public–private sector cooperation.

The solutions proposed in the Cybersecurity Strategy are more clearly oriented towards protecting *cyberspace*, an aim explicitly articulated in the Strategy's definition of cybersecurity:

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

The way in which the Strategy's efforts centres around the protection of cyberspace and its interconnected networks is further illustrated in the following quote: "Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace." (European Commission, 2013a, p. 2). The Cybersecurity Act does not engage explicitly with the protection of cyberspace but emphasises non-human referent objects within it. It proposes taking all necessary actions to "improve cybersecurity in the Union so that network and information systems, communications networks, digital products, services and devices used by citizens, organisations and businesses (…) are better protected from cyber threats." (Regulation (EU) 2019/881). By protecting these objects, it is stated, the risks faced by individuals and by society as a whole will be mitigated.

The vulnerability of children problematisation

The third problem representation refers to the *vulnerability of children* in online environments. The Cybersecurity Strategy speaks of specific actions to combat child sexual abuse and exploitation (CSA/CSE) online through legislative measures and encourages member states to take further actions with support from the Commission and the EC3. As articulated in the Cybersecurity Act, children are to be seen as particularly "vulnerable persons" (Regulation (EU) 2019/881). The problematisation stands out as it singles out the protection of a particular group – children. Thus, it stands in contrast to the first problem representation by referring to the security of a different referent object. The exceptionality of the vulnerability of children problematisation is highlighted in the 2017 SOCTA report, which states that "[w]hile neither offline nor online CSE meet the criteria to be considered 'organised crime' this is still a high priority crime due to the degree of physical and psychological damage to one of society's most vulnerable groups – children." (Europol, 2017b, p. 31). There is an emphasis on the moral necessity of protecting children. This is evident from the emotive language used when referring to CSE, which is described in terms such as "abhorrent", "heinous" and "perverse".

The end-user behaviour problematisation

Because children are considered a particularly vulnerable group, efforts are directed towards protecting them. There is, however, an element of friction to be found here. While in general, children are conceived as victims, there are segments in the analysed texts in which children are constructed as responsible for their victimisation: "By exposing their personal details online without proper precautions, either via social media platforms or by sharing sexualised self-produced images, children and adolescents create the possibility of being targeted as potential victims by online predators." (Europol, 2014, p. 30). The 2019 IOCTA also states that "there is a growing number of minors sharing sexual pictures or videos with peers. Children are making themselves vulnerable on a number of levels through this behaviour, including in the context of online solicitation by child sexual offenders." (Europol, 2019, p. 32). Awareness-raising of CSA is a reoccurring feature in the cybercrime policies. For example, the documents state the need to "raise awareness and provide children with tools to protect themselves" (Europol, 2016, p. 25). The #SayNo campaign, which aims to educate young people on the risk of being subjected to sexual coercion and extortion online, is a concrete example of efforts to change the behaviour of current or potential victims (Europol, n.d.a). Europol provides cautionary advice for young people to avoid being abused online such as the following: “Abusers look for young people who use a sexualised username, post sexualised pictures or talk about sex online. Think about how your online profile makes you appear to others.” (Europol, n.d.b). Raising awareness of cybersecurity risks among end-users is an integrated part of the wider cybersecurity policies too. For example, the Cybersecurity Strategy states that “[end users] need to be made aware of the risks they face online and be empowered to take simple steps to guard against them.” (European Commission, 2013a, p. 8).

5.2. What deep-seated conceptual logics underlie this representation of the “problem”?

The control of cyberspace logic

The non-human referent object problematisation is underpinned by two conceptual logics. The first is the control of cyberspace logic. It corresponds to a logic found in traditional security discourse – that of protecting the nation-state. As the protection must be understood as a relationship of power in which the protector control’s those he protects, this logic centres around control (Stiehm, 1982). Although cyberspace, unlike territory, is a form of space that is not marked by geographical boundaries, the functioning of the control logic within the two domains is in some ways similar. Much like the nation-state’s territorial control, which largely justifies the nation-state’s existence, the control of cyberspace logic is about the control of space. Protecting the referent object of security (be it the nation-state or cyberspace) involves a construction of the protected actors within it as subjects without agency (Kronsell, 2016). The control logic is gendered and connected to the notion of hegemonic masculinity. As Garlick describes it, “being a man” means being in control (Garlick, 2010). In the control of cyberspace logic, the nation-state, which is the referent object of security in the traditional security discourse, is replaced by cyberspace as the object which the masculine protector must defend.

The technical logic

The aim to protect networks, information systems, ICT products, devices and services from cyber threats is underpinned by a logic I would call the technical logic. It suggests that individual and societal vulnerabilities can be reduced if for example networks, information systems and ICT products are better protected from cyber threats. For example, the Cybersecurity Act proposes that the introduction of certification schemes for ICT products, services and processes and security-by-design practices can mitigate the cybersecurity risks faced by citizens, businesses and organisations. As previous research has suggested, a technical approach to global issues is often associated with a masculinised form of governance (Kronsell

& Magnusdottir, 2015). It is stated that a technical approach does little in terms of addressing gendered issues stemming from underlying gender inequality. Thus, it has a tendency to depoliticise governance, rendering issues of gender silent (Bondesson, 2019).

The vulnerability of children logic

The third logic constructs children's victimisation to online sexual exploitation as a societal concern because of their position as "one of society's most vulnerable groups" (Europol, 2017b, p. 31). Here, a protection-protected notion can be found in which children embody the perfect form of vulnerability for the masculine protector to protect and guide. I suggest that this protector is a sort of paternal defender, reminiscent of Young's (2003) masculine household protector. It is a loving form of protection which does not aim for suppression, but nevertheless expects gratefulness and passivity from the protected vulnerable. In the vulnerability of children logic, the protector can expect obedience from the protected vulnerable because children, due to their generally accepted status as passive "recipients of adult protection" (Lansdown, 2001, p. 1) rather than subjects of rights with their own political voices (O'Neill & Zinga, 2008, p. 17). Children as the protected vulnerable, therefore, cannot and do not question the masculine protector's authority. As Young explains, the masculine protection notion can both feminize and infantilize the protected (2003). The vulnerable children, then, perfectly embody the infantilized protected.

The end-user responsibility logic

The logic underpinning the end-user behaviour problematisation is the end-user responsibility logic. According to this logic, end-users can avoid becoming victims of cyber-crimes by taking responsibility for their online presence and avoid exposing themselves to risks. Therefore, education for end-users is considered an effective way to fight such crimes. This is reminiscent of a logic which is familiar within feminist research and commonly referred to as "victim blaming". For example, discourses on rape are frequently focused on the behaviour of the victim – walking alone in public spaces, accompanying the perpetrator to their house, dressing in provocatively or being sexually active – thus shifting the blame for the rape from the perpetrator to the victim (Chancer, 2009).

This logic is particularly salient in segments dealing with online child sexual coercion and extortion. There seem to be an implicit assumption about the victims of such crimes, as compared to other forms of CSE. Looking at images and language used to depict the potential victims of sexual coercion and extortion, they are portrayed as older, wearing make-up and described as sexually explicit in their online activity (Europol, n.d.a; n.d.b). This stands in stark contrast to images otherwise used in the context of CSE. For example, the 2018 IOCTA, in relation to a segment on CSE, portrays an image of a young child in front of a computer screen with a teddy bear in her lap (Europol, 2018, p. 33). What can be seen as implicitly stated in these representations is an assumption that there is a difference between innocent, young children who must be protected (as described in the vulnerability of children logic) and adolescents who make themselves vulnerable by, for example, expressing their sexuality online.

5.3. What is left unproblematic in this problem representation? Where are the silences? Can the "problem" be conceptualised differently?

The control of cybersecurity logic has a key feature which makes the incorporation of a gender perspective more difficult. Critical feminist perspectives have emphasised that a gender-sensitive concept of security must start from women's everyday experiences and link them with broader political structures and processes (Hudson, 2005). However, lived experiences are not consulted in a security discourse which aims for the security of cyberspace – not the security of individuals and groups operating within it. Only by acknowledging that the sources of (in)securities differ across intersecting identity factors such as gender can they be understood and countered. Such considerations are omitted in traditional, statist conceptualisations of security (Tickner, 1992).

The technical logic, which proposes that societal and individual vulnerabilities can be reduced by improving the security in ICT products, networks and information systems, also has a characteristic which makes it incompatible with a gender-sensitive concept of cybersecurity. As Hansen and Nissenbaum (2009) argue, insecurities of networks and information infrastructure often also result in insecurities for individuals. However, technology-facilitated violence against women does not necessarily stem from what we normally consider technological vulnerabilities. An offender can use multiple different online tools to victimise women, without having to take advantage of exploits and technological security flaws. For example, hate speech, online harassment and non-consensual pornography are forms of violence which are not necessarily dependent on these kinds of vulnerabilities. Protecting networks, ICT products and information infrastructure from cyber threats is therefore not sufficient for addressing women's insecurities. This is not to say that programmes cannot be developed in ways which serve to reduce women's vulnerabilities. Slupska (2019), for example, argues for the employment of "access control" to address issues such as non-consensual pornography. Much like a company employee loses access to sensitive files when leaving the company, programmes could be developed in which access to intimate material can be revoked when a relationship ends, or consent is otherwise withdrawn. A similar project has been attempted by Facebook, in which users can send intimate images, have them converted by the company into a unique digital fingerprint, and use that fingerprint to identify and block unwanted attempts to redistribute the image (Solon, 2017). What is clear is that protecting information, networks and machines is not the same as protecting the humans who use them. A feminist approach to cybersecurity must therefore begin with a focus on protecting humans from harm, with gendered issues in mind.

The third logic is the vulnerability of children logic. Although presented as an ungendered problem in the EU documents, CSA is a gendered issue. According to INHOPE statistics, 97% of all reported CSA material in 2017 depicted girls (INHOPE, 2017). As for the offenders of online-facilitated CSA, evidence suggest that perpetrators are predominantly men and primarily from a Caucasian or European background (Finkelhor & Ormrod, 2004; Aslan & Edelmann, 2014; Tener, Wolak and Finkelhor 2015). The examined documents, however, fail to account for the gendered nature of this kind of violence. This is mirrored in policy problem representations of "domestic violence", which have a tendency to marginalise the connection between violence and masculinity and the fact that most perpetrators are men (Hearn & McKie 2010). In the same way, the end-user responsibility logic focuses solely on the potential victims of cybercrime. Instead of only educating potential victims, increased efforts could be directed towards reaching potential perpetrators and providers of abuse tools. Education on digital ethics which includes gender and human rights perspectives could be implemented as a preventive measure. Furthermore, raising awareness about the harmful effects of cyber violence on victims could contribute to increasing the status of such issues. As indicated by previous research, intimate partner cyber-stalking "is largely perceived to be less serious and less deserving of survivor support" than physical forms intimate partner violence (Messinger, Birmingham & Dekeseredy, 2018, p. 1). It should be noted that one document does mention gender as a factor in cybercrime. It does so when describing victim and perpetrator "profiles" of child sexual extortion and coercion. However, even in this instance (which covers only one crime area), the text does not engage further in the gendered nature of violence and the structural mechanisms underpinning VAWG.

The vulnerability of children logic can also help in understanding how children can be constructed as a vulnerable group, while women are not. What differentiates children's vulnerability from that of other vulnerable groups is that children's vulnerability can be seen as inherent – children are vulnerable because they are children. In contrast, women's vulnerability is best understood as a product of structural gender inequality, at least from a contemporary feminist point of view. Singling out children as a particularly vulnerable group, therefore, does not necessarily render the need to examine security issues specific to other groups, because their vulnerability is not nature-given. Thus, this logic makes it possible to omit women's security issues and the societal factors which constitute the source of their vulnerability.

Even at the EU level, there are competing understandings of cybersecurity issues, including problematisations which incorporate a gender perspective. The European Parliament has, through the adoption of several resolutions, attempted to bring issues of cyber violence to the EU's cybersecurity agenda. For example, suggestions have been made to redefine "public space" in a way that also includes virtual spaces such as websites and networks (European Parliament, 2018c), construct legal definitions of those forms of cyber VAWG that are not yet legally recognised (European Parliament, 2018a) and enhance the availability of data on cyber VAWG at the EU level (European Parliament, 2018b). In terms of EU level advocacy, the European Women's Lobby (2017) has argued for integrating gendered forms of cybercrime into the institutions and agencies working with combatting cybercrime.

5.4. What effects are produced by this representation of the "problem"?

There is an inherent risk in excluding gendered security issues in cybersecurity and -crime policy. By silencing gendered security issues, the responsibility for women's victimisation is shifted onto themselves. This is reflected in the individualisation of gendered security issues which previous feminist research has identified (Slupska, 2019; True, 1995). A possible discursive effect of this is that women's victimisation is seen as the result of their own naïveté, feeding into a larger context of "victim blaming", in which the behaviour of the victim is subjected to more public scrutiny than the actions of the perpetrators. As earlier research has demonstrated, victim blaming attitudes is a factor that contributes to creating a violence-accepting climate (Gracia & Tomás, 2014). Feelings of shame and guilt are also a commonly reported reason as to why victims of sexual violence decide not to report to the police (Ceelen et al. 2019). Furthermore, earlier research suggests that online "trolling" (e.g. death threats, rape threats and body shaming) can be seen as examples of "silencing strategies" which attempt to remove women from participation in online public spaces. Lumsden and Morgan suggest that by focusing on victim behaviour in regard to cyber VAW, public discourses tend to reinforce these "silencing strategies" (Lumsden & Morgan, 2017). In the same way, policies which leave women responsible for their own security online risks pushing women out of virtual public spaces, as indicated by the survey study published by Amnesty International (2017). The lived effects of a genderblind conceptualisation of cybersecurity and -crime can thus include self-censorship and digital exclusion of women in online spaces (Van Der Wilk, 2018). Conceptualising violence as a result of women's naïveté also draws attention away from the perpetrators of violence and the structural mechanisms underpinning violence against women. As women's activists have cautioned, insufficient political action against gendered cybercrime risks contributing to a naturalisation of violence against women, allowing perpetrators to continue the abuse of women and girls (European Women's Lobby, 2017).

A possible discursive effect of the institutional focus on protecting cyberspace and the products, services, networks and information therein is that cyber threats and risks are seen as separate phenomena from "real-world" phenomena. By closing off "cyberspace" as a unit of interest, the full extension of the practices and patterns which transcend the online-offline boundaries are not grasped. In regard to gendered technology-facilitated security issues, this means that cyber violence is not discursively fitted into the larger continuum of men's violence against women. As Lewis, Rowe and Wiper argues, online abuse should be understood as "an extension of offline gender relations which are marked by abuse and VAWG." (Lewis, Rowe & Wiper, 2017, p. 1463). Previous research has for example identified that cyber sexual harassment co-occurs with traditional sexual harassment (Leemis et al., 2019) and argued that online sexual violence should be understood, not as an exceptional phenomenon, but as existing on a continuum with other forms of sexual violence (McGlynn Rackley & Houghton, 2017). Cyber harassment and violence against women often reflect offline victimisation, which is extended or even amplified through technological means. An extreme empirical example is November 2, 2018 in Tallahassee when a 40-year-old man walked into a yoga studio and killed two women before taking his own life. Before the crime, the perpetrator had openly expressed a hatred against women and a desire to do harm online (Richter & Richter, 2019). Even though there are reasons for acknowledging the distinctive features of cyberspace (see Dunn Cavelty, 2012; 2013), it is also important to highlight that the activities in cyberspace are part of a larger context. Some segments engaging with the issue of CSE make the connection between online and offline perpetration by for example stating that a number of offenders in possession of CSEM are also involved in offline sexual exploitation. However, the analysis of the connections between online and offline perpetration does not go beyond acknowledging its existence and does not incorporate a recognition of its place in global gender relations.

Lastly, promoting technical solutions gives primacy to male-dominated professions in countering cybersecurity and -crime "problems", which is relevant for the question of which actors will benefit from such efforts. Because STEM professions, including cybersecurity professions, are dominated by male bodies, many of the proposed solutions will be carried out in fields dominated by men. This means that technical solutions to cybersecurity issues are not gender neutral, because the ones who control decisions in technology are predominantly men (Kronsell, 2013). As such, we can also understand the technical logic in relation to the intimate connection between technology and the masculinisation of power, in which technology is deeply institutionalised as a masculine domain (See Cockburn, 1985; Mellström & Holdt, 2011). By focusing on technical solutions and innovations, the efforts to counter cybersecurity "problems" remains in a masculinised realm. Given that technologies which are developed by homogenous groups of people often end up reflecting the biases of those groups (Harding, 1991), such technical solutions could also end up contributing to a reproduction of discrimination, prejudice and masculine ideals – if emphasis is not put on integrating diverse perspectives.

6. Discussion

6.1. Limitations

This thesis has specifically focused on issues of cybercrime and it is important to note that the findings from this study do not necessarily correspond to the dynamics of the other cybersecurity pillars. The EU's efforts relating to cyber issues are also not restricted to cyber*security* efforts. There are also policies within the more general area of cyber which this thesis has not engaged with. Another limitation which should be highlighted is that the examined documents were published between 2014 and 2019 but exploring changes over time was not included in the aim of this thesis. It is therefore possible that the examined institutions may have undergone institutional changes during these years which this analysis has not accounted for.

6.2. Conclusions

In this thesis I conducted an analysis of the EU's cybersecurity and -crime institutions, which are marked by genderblind conceptualisations of cybersecurity and -crime issues. To explore and critically reflect on this, I applied a theoretical perspective based on feminist institutionalism and path dependence and used Carol Bacchi's post-structural WPR approach to interrogate relevant texts. The aim of the thesis was to explore what conceptual logics make it possible for the EU to conceptualise cybersecurity and -crime “problems” in a genderblind way, despite women being disproportionally subjected to certain forms of technology-facilitated violence. Four such logics were identified:

- The control of cyberspace logic, which positions cyberspace as the referent object of security, omits women’s everyday experiences and the differing sources of (in)securities among different identity factors.
- The technical logic proposes that the risks faced by individuals and societies can be mitigated by increasing the security of ICT products, processes and services. This logic overlooks gendered technology-facilitated security issues as it is grounded in a focus on protecting products, processes and services from harm – not humans.
- The vulnerability of children logic constructs children as a vulnerable group whose victimisation is morally necessary to counter. It renders the gendered nature of CSE silent and makes it possible to neglect women’s experiences because it does not engage with societally produced vulnerabilities.
- The end-user responsibility logic assumes that some forms of crimes are best countered by changing the behaviours of the victims. This logic shifts focus from the perpetrators to the victims, silencing the connection between violence and masculinity.

These logics are complex and somewhat contesting. For example, some logics emphasise different referent objects (human or non-human) and construct different kinds of subject (vulnerable or risk-taking). The possible effects (discursive, subjectification and lived effects) of the identified problematisations have been discussed – including the risk of contributing to a naturalisation of violence against women, self-censorship and digital exclusion of women in online spaces and insufficient political actions against gendered cyber issues, allowing perpetrators to continue the abuse of women and girls.

While conducting my analysis, I took help of previous research, in particular feminist scholarship engaging with issues of gender, security and technology. The identified conceptual logics all have features which are mirrored in previous findings. As stated earlier, FI would suggest that the prevalence of masculinised logics within other security domains (Kronsell, 2016; Ericson, 2018a; 2018b) as well as the dominance of male bodies and masculine biases in technology (Cockburn, 1985; EIGE, 2018; Peacock & Irons, 2017) has created path dependence for how the emerging field of cybersecurity can be understood. In regard to this, the findings from the analysis suggest gendered path dependence which privileges masculinised ways of understanding cybersecurity and -crime issues.

This thesis contributes to cybersecurity scholarship, which is generally lacking in feminist research. In particular, previous research has not investigated discursive hindrances to the incorporation of gender perspectives in cybersecurity policy. I have also demonstrated that applying a WPR approach is fruitful for exploring the absence of gender in policy. Feminist scholars have predominantly used WPR to analyse gender-related policy, with some exceptions (see Bondesson, 2019). The analysis also contributes to feminist IR scholarship by relating the findings to previous studies, particularly on gender and security. The findings suggest that the field of cybersecurity and -crime is on a path of reproducing dynamics found in other security domains. For example, the emphasis on protecting non-human referent object of security and the focus away from the perpetrators are mirrored in previous research on gender and security.

A final contribution of this thesis is to make suggestions on how a gender-sensitive conceptualisation of cybersecurity and -crime "problems" could be conceived. The analysis suggests that a gender-sensitive conceptualisation of cybersecurity and -crime issues should:

- Start from women's everyday experiences;
- Be grounded in a focus on protecting humans from harm;
- Include an understanding of gendered cybersecurity and -crime issues as part of a continuum of perpetrations committed against women;
- Acknowledge the sources of women's vulnerability and victimisation as underpinned by structural gender inequality.

Given the speed at which the domain of cybersecurity is growing, it should be of particular importance that the conceptualisations of cybersecurity and -crime issues are not constructed without critical reflections. As the findings from this thesis suggest, the logics underpinning problematisations of cybersecurity and -crime issues have consequences for what policy and strategy options are being proposed, which in turn impact the lives of people. Because the cybersecurity sector growing exponentially, policymakers should keep the suggestions of path dependence in mind – that when certain understandings of cybersecurity and -crime issues become institutionalised in cybersecurity institutions, they become difficult to break from. As Bacchi (2009) argues, the conceptual logics which underpin legislations and other instruments used to govern are especially important, because these understandings "stick". This points to the need for critical, feminist perspectives on cybersecurity and -crime policy, which this thesis has contributed with.

Lastly, I would like to suggest that further research should be conducted which applies feminist perspectives to cybersecurity. The scope of this thesis has not allowed for further investigation into how the genderblind problematisations of cybersecurity and -crime issues have come about. For example, interviews with policymakers in EU institutions would provide deeper understandings of the observed phenomenon by looking at its genealogy. As mentioned earlier, other actors, such as the European Women's Lobby and the European Parliament have argued for more gender-sensitive understandings of cybersecurity. As such, it could be useful to apply a framing analysis (Björnehed & Erikson, 2018), comparing the frames of different actors at the European level. It would also be interesting to conduct studies into the other pillars of EU's cybersecurity. The area of cyber-defence is particularly interesting due to its military connotations and the network and information security pillar because it deals with the protection of critical infrastructure and thus has a connection to national security. Both military institutions and national security discourses are subjects which have been previously explored by feminist scholars (see for example Kronsell, 2016; Tickner 1992), and their extensions into the cyber domain should therefore be of interest for feminist research. Studies on cybersecurity and gender outside the EU should also be encouraged.

Literature

Ackerly, B. A., Stern, M. and True, J. (2006). *Feminist Methodologies for International Relations.* Cambridge: Cambridge University Press.

Amnesty International (2017). *Amnesty reveals alarming impact of online abuse against women*. [online] Retrieved 7 January 2020 from https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/

Aslan, D. and Edelmann, R. (2014). Demographic and offence characteristics: a comparison of sex offenders convicted of possessing indecent images of children, committing contact sex offences or both offences. *The Journal of Forensic Psychiatry & Psychology, 25*(2), 121-134.

Bacchi, C. (2009). *Analysing Policy: What's the problem represented to be?* Frenchs Forest: Pearson Education.

Bacchi, C., & Goodwin, S. (2016). *Poststructural policy analysis: A guide to practice*. New York: Palgrave Pivot.

Björnehed, E, & Erikson, J. (2018). Making the most of the frame: Developing the analytical potential of frame analysis. *Policy Studies, 39*(2), 109-126.

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

Bondesson, S. (2019). Why Gender Does Not Stick: Exploring Conceptual Logics in Global Disaster Risk Reduction Policy. In Kinvall, C. & Rydström, H (eds). *Climate Hazards, Disasters, and Gender Ramifications*. Routledge, 88-124.

Bretherton, C. (2001). Gender mainstreaming and EU enlargement: Swimming against the tide? *Journal of European Public Policy, 8*(1), 60-81.

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

Buzan, B. (1991) New patterns of global security in the twenty-first century. *International Affairs 67*(3).

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

Cavaghan, R. (2017). *Making Gender Equality Happen: Knowledge, Change and Resistance in EU Gender Mainstreaming*. New York: Routledge.

CCDCOE (n.d.). EU Data Retention Directive Invalid. [online] Retrieved 7 January 2020 from https://ccdcoe.org/incyder-articles/eu-data-retention-directive-invalid/

Ceelen, M., Dorn, T., Van Huis, F., & Reijnders, U. (2019). Characteristics and Post-Decision Attitudes of Non-Reporting Sexual Violence Victims. *Journal of Interpersonal Violence, 34*(9), 1961-1977.

Chancer, L. (2009). Victim Blaming Through High-Profile Crimes: An Analysis of Unintended Consequences. Humphries, D. (ed). *Women, violence, and the media readings in feminist criminology*. Boston: Northeastern University Press, 256-268.

Christou, G. (2019). The collective securitisation of cyberspace in the European Union. *West European Politics, 42*(2), 278-301.

Cockburn, C. (1985) *Machinery of Dominance: Women, Men and Technical Know-how*. London: Pluto Press.

Council of the European Union (2018). *The EU Policy Cycle to Tackle Organised and Serious International Crime.* Retrieved 7 January 2020 from https://www.consilium.europa.eu/media/37340/20185274_qc0418775enn_pdf.pdf

Deibert, R. (2018). Trajectories for Future Cybersecurity Research. In Gheciu, A. & Wohlforth, W. (eds), *The Oxford Handbook of International Security* [e-book]. Oxford: Oxford University Press.

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

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review, 15*(108), 105-122.

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities. *Science and Engineering Ethics, 20*(3), 701-715.

Eaton, A., Jacobs, H., & Ruvalcaba, Y. (June 2017). *2017 Nationwide online study of nonconsensual porn victimization and perpetration*. Cyber Civil Rights Initiative. [report] Retrieved 7 January 2020 from https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf

EIGE (19 June 2017). *Cyber violence is a growing threat, especially for women and girls.* [online] Retrieved 7 January 2020 from: https://eige.europa.eu/news/cyber-violence-growing-threat-especially-women-and-girls

EIGE (2017). Cyber Violence Against Women and Girls. [report] Retrieved 7 January 2020 from https://eige.europa.eu/publications/cyber-violence-against-women-and-girls

EIGE (2018). *Study and work in the EU: Set apart by gender.* [report] Retrieved 7 January 2020 from https://eige.europa.eu/publications/study-and-work-eu-set-apart-gender-report

Ericson, M., (2018a). *Genus, risk och sårbarhet: en populärvetenskaplig sammanfattning av resultat från ett postdoktoralt forskningsprojekt*. Myndigheten för samhällsskydd och beredskap.

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

European Commission, (1996). *Incorporating Equal Opportunities for Women and Men into All Community Policies and Activities*. COM (96), 67 Final. Retrieved 16 December 2019 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ac10921

European Commission (2015). The European Agenda on Security. COM (2015) 185 Final. Retrieved 7 January 2020 from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

European Commission (2017). *Europeans' Attitudes Towards Cyber Security.* [report] Retrieved 7 January 2020 from https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171

European Commission (2019). *The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification*. [online] Retrieved 7 January 2020 from https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity

European Commission (n.d.) *Say No! Stop Violence Against Women*. [online] Retrieved 7 January 2020 from https://ec.europa.eu/justice/saynostopvaw/about.html

European Parliament (2017). *European Parliament resolution of October 2017 on the fight against cybercrime.* Retrieved 7 January 2020 from http://www.europarl.europa.eu/doceo/document/TA-8-2017-0366_EN.html?redirect

European Parliament (2018a). *European Parliament resolution of 17 April 2018 on empowering women and girls through the digital sector*. Retrieved 7 January 2020 from http://www.europarl.europa.eu/doceo/document/TA-8-2018-0102_EN.html?redirect

European Parliament (2018b). *Resolution of 17 April 2018 on gender equality in the media sector in the EU.* Retrieved 7 January 2020 from http://www.europarl.europa.eu/doceo/document/TA-8-2018-0101_EN.html?redirect

European Parliament (2018c). *Resolution of 11 September 2018 on measures to prevent and combat mobbing and sexual harassment at workplace, in public spaces, and political life in the EU.* Retrieved 7 January 2020 from http://www.europarl.europa.eu/doceo/document/TA-8-2018-0331_EN.html

European Women's Lobby (2017). #HerNetHerRights. Mapping the State of Online Violence Against Women & Girls in Europe. Retrieved 7 January 2020 from https://www.womenlobby.org/IMG/pdf/hernetherrights_report_2017_for_web.pdf

Finkelhor, D., & Ormrod, R. (2004). *Child pornography: Patterns from NIBRS.* Juvenile Justice Bulletin. Office of Justice, US Department of Justice. [report] Retrieved 7 January 2020 from https://www.ncjrs.gov/pdffiles1/ojjdp/204911.pdf

FRA (2015). *Violence Against Women: An EU-wide Survey. Main Results*. Luxembourg: Publications of the European Union. [report] Retrieved 7 January 2020 from https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

Garlick, S. (2010). Taking Control of Sex? Hegemonic Masculinity, Technology, and Internet Pornography. *Men and Masculinities, 12*(5), 597-614.

Gracia, E., & Tomás, J. (2014). Correlates of Victim-Blaming Attitudes Regarding Partner Violence Against Women Among the Spanish General Population. *Violence Against Women, 20(*1), 26-41.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175.

Harder, H. (2010). Explanatory Case Study. In Mills, A., Durepos, G., & Wiebe, E. (eds), *Encyclopedia of Case Study.* London: SAGE, 370-371.

Harding, S. (1991). *Whose Science? Whose Knowledge? Thinking from Women's Lives*. Ithaca: Cornell University Press.

Hearn, J. & McKie, L. (2010). Gendered and social hierarchies in problem representation and policy processes: "domestic violence" in Finland and Scotland. *Violence against Women,16*(2), 136-158.

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

Hutchings, K. (2008). Making Sense of Masculinity and War, *Men and Masculinities 10*(8), 389-404.

INHOPE (2017). *Statistic 2017*. [online] Retrieved 7 January 2020 from http://88.208.218.79/tns/resources/statistics-and-infographics/statistics-and-infographics-2017.aspx

Holm, M. (2019). *The Rise of Online Counterpublics? The Limits of Inclusion in a Digital Age.* Uppsala: Department of Government. [dissertation]

Kasper, A. (2014). The Fragmented Securitization of Cyber Threats. In Kerikmäe, T. (ed) *Regulating eTechnologies in the European Union.* Springer International Publishing, 157-187.

Khalili, L. (2011). Gendered practices of counterinsurgency. *Review of International Studies, 37*(4), 1471-1491.

Kronsell, A. (2016). Sexed Bodies and Military Masculinities: Gender Path Dependence in EU's Common Security and Defense Policy. *Men and Masculinities 19*(3), 311-336.

Kronsell, A. & Magnusdottir. G. (2015) The (In)Visibility of Gender in Scandinavian Climate Policy-Making. *International Feminist Journal of Politics 17*(2), 208–326.

Lansdown, G. (2001). *Promoting Children's Participation in Democratic Decision-making.* Florence: UNICEF. Retrieved 7 January 2020 from https://www.unicef-irc.org/publications/pdf/insight6.pdf

Le Bail, K. (2018) *John Cage, or chance as a discipline*. [online] Retrieved 7 January 2020 from http://www.diptyqueparis-memento.com/en/john-cage-or-chance-as-a-discipline/

Leemis, R., Espelage, D., Basile, K., Mercer Kollar, L., & Davis, J. (2019). Traditional and cyber bullying and sexual harassment: A longitudinal assessment of risk and protective factors. *Aggressive Behavior, 45*(2), 181-192.

Lewis, R., Rowe, M., & Wiper, C. (2017). Online Abuse of Feminists as An Emerging form of Violence Against Women and Girls. *British Journal of Criminology, 57*(6), 1462-1481.

Lowndes, V. (2010) The Institutional Approach. In Marsh, D. and Stoker, G. (eds) *Theory and Methods in Political Science*, 3rd ed. Houndmills: Palgrave Macmillan, 60-79.

Lumsden, K. & Morgan, H (2017). Media framing of trolling and online abuse: silencing strategies, symbolic violence, and victim blaming. *Feminist Media Studies, 17*(6), 926-940.

Mackay, F., Kenny, M. & Chappell, L. (2010). New Institutionalism Through a Gender Lens: Towards a Feminist Institutionalism? *International Political Science Review, 31*(5), 573-588.

Masters, C. (2009). Femina Sacra: The `War on/of Terror', *Women and the Feminine. Security Dialogue, 40*(1), 29-49.

McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse. *Feminist Legal Studies, 25*(1), 25-46.

Mellström, U. & Holth, L. (2011). Revisiting Engineering, Masculinity and Technology Studies: Old Structures with New Openings" *International Journal of Gender, Science, and Technology*, *3*(2), 313-329.

Messinger, A., Birmingham, R., & Dekeseredy, W. (2018). Perceptions of Same-Gender and Different-Gender Intimate Partner Cyber-Monitoring. *Journal of Interpersonal Violence*, 1-21.

Mohammed, S., Peter, E., Gastaldo, D. & Howell, D. (2015). Rethinking Case Study Methodology in Poststructural Research. *Canadian Journal of Nursing Research, 47*(1), 97-114.

Narain, S. (2014). Gender in International Relations: Feminist Perspectives of J. Ann Tickner. *Indian Journal of Gender Studies, 21*(2), 179-197.

O'Neill, T. & Zinga, D. (2008). Introduction. In O'Neill, T. & Zinga, D. (eds). *Children's rights multidisciplinary approaches to participation and protection.* Toronto: University of Toronto Press, 3-18.

Papademetriou, T. (2014). European Union: ECJ Invalidates Data Retention Directive. [report] Retrieved 7 January 2020 from https://www.loc.gov/law/help/eu-data-retention-directive/eu-data-retention-directive.pdf

Peacock, D. & Irons, A. (2017). Gender Inequality in Cybersecurity: Exploring the Gender Gap in Opportunities and Progression. *International Journal of Gender, Science and Technology 9*(1), 25-44.

Pew Research Center (October 2014). Online Harassment. [report] Retrieved 7 January 2020 from http://www.pewinternet.org/2014/10/22/online-harassment/

Richter, G. & Richter, A. (March 2019). *The Incel Killer and the Threat to the Campus Community*. Security Magazine. [online] Retrieved 7 January 2020 from https://www.securitymagazine.com/articles/89962-the-incel-killer-and-the-threat-to-the-campus-community

Shortt, Denise M. (1998). Gender and technology: Looking to the past. *Canadian Woman Studies, 17*(4).

Shirin, M. & Waylen, G. (2008). Introduction: Feminist Perspectives on Analysing and Transforming Global Governance. In Shirin, M. & Waylen, G. (eds.) *Global Governance: Feminist Perspectives*. Basingstoke: Palgrave Macmillan, 1-18.

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

Staude-Müller, F., Hansen, B. & Voss, M. (2012). How stressful is online victimization? Effects of victim's personality and properties of the incident. *European Journal of Developmental Psychology, 9*(2), 260-274.

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

Stratigaki, M. (2005). Gender Mainstreaming vs Positive Action: An Ongoing Conflict in EU Gender Equality Policy. *European Journal of Women's Studies, 12*(2), 165-186.

Sylvester, C. (2013). *War as experience: Contributions from international relations and feminist analysis*. London: Routledge.

Tener, D., Wolak, J. and Finkelhor, D. (2015). A typology of offenders who use online communications to commit sex crimes against minors. *Journal of Aggression, Maltreatment & Trauma, 24*(3), 319-337.

Trifonov, S. (2017). Performing Prudence: Barack Obama's Defense of NSA Surveillance Programs. *Advances in the History of Rhetoric, 20*(1), 28-46.

Solon, O. (2017). *Facebook asks users for nude photos in project to combat 'revenge porn'*. The Guardian. [online] Retrieved 7 January 2020 from https://www.theguardian.com/technology/2017/nov/07/facebook-revenge-porn-nude-photos

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

Tickner, A. (2002). Feminist Perspectives on 9/11. *International Studies Perspectives 3*(4), 333-350.

True, J. (1995). Feminism. In Burchill, S. (ed) *Theories of International Relations*. New York: St. Martin's Press, 216-234.

True, Jacqui. (2003). Mainstreaming Gender in Global Public Policy. *International Feminist Journal of Politics,* 5(3), 368-396.

Van Der Wilk, A. (2018). *Cyber violence and hate speech online against women*. European Parliament. Retrieved 7 January 2020 from http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

Walby, S. (2005). Introduction: Comparative gender mainstreaming in a global era. *International Feminist Journal of Politics, 7*(4), 453-470.

Young, I. (2003). The Logic of Masculinist Protection: Reflections on the current security state. *Signs: Journal of Women in Culture and Society, 29*(1), 1-25.

Young, I. (2007). *Global Challenges. War, Self-determination and Responsibility for Justice.* Cambridge: Polity Press.

(2017) The WannaCry ransomware attack. *Strategic Comments, 23*(4), vii-ix.

Empirical material

EC3 (2014). *First Year Report*. Retrieved 6 January 2020 from https://www.europol.europa.eu/publications-documents/european-cybercrime-center-ec3-first-year-report

European Commission (2013a). *EU cyber security strategy: An open, safe and secure cyberspace*. JOIN (2013). 01 Final. Retrieved 7 January 2020 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001

European Commission (2013b). *Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre.* COM (2012) 140 Final. Retrieved 7 January 2020 from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0140

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Retrieved 2 January 2020 from https://eur-lex.europa.eu/eli/reg/2019/881/oj

Europol (2013). *The European Union (EU) Serious and Organised Crime Threat Assessment.* Retrieved 7 January 2020 from https://www.europol.europa.eu/activities-services/main-reports/eu-serious-and-organised-crime-threat-assessment-socta-2013

Europol (2014). *The Internet Organised Crime Threat Assessment*. Retrieved 2 January 2020 from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014

Europol (2015). *The Internet Organised Crime Threat Assessment*. Retrieved 2 January 2020 from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015

Europol (2016). *The Internet Organised Crime Threat Assessment*. Retrieved 2 January 2020 from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

Europol (2017a). *The Internet Organised Crime Threat Assessment*. Retrieved 2 January 2020 from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

Europol (2017b). *The European Union (EU) Serious and Organised Crime Threat Assessment.* Retrieved 2 January 2020 from https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

Europol (2017c). *Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective.* Retrieved 2 January 2020 from https://www.europol.europa.eu/publications-documents/online-sexual-coercion-and-extortion-form-of-crime-affecting-children-law-enforcement-perspective

Europol (2018). *The Internet Organised Crime Threat Assessment*. Retrieved 2 January 2020 from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

Europol (2019). *The Internet Organised Crime Threat Assessment*. Retrieved 2 January 2020 from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Europol (n.d.a). *Online Child Sexual Coercion and Extortion is a Crime.* [online] Retrieved 7 January 2020 from https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime

Europol (n.d.b). *Your Life is Online. Protect it!* [online] Retrieved 7 January 2020 from https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/your-life-online-protect-it