FEMINIST ENCOUNTERS
A JOURNAL
OF CRITICAL STUDIES
IN CULTURE AND POLITICS

Feminist Encounters: A Journal of Critical Studies in Culture and Politics, 9(2), 25
ISSN: 2468-4414

lectito

A Feminist Critique of Cybersecurity: Technofeminist Imaginaries of Vulnerability and Care

nate wessalowski [1]*, Grit Marti Lange [2], Sigrid Kannengießer [1]

Published: September 1, 2025

ABSTRACT

The internet, in its commercialised and increasingly centralised form, is not safe, particularly for women and non-binary and trans people affected by intersectional patterns of discrimination and oppression. In this article, we investigate how cybersecurity can mitigate or contribute to gendered experiences of insecurity. As a field of practices, discourses and tools, cybersecurity is currently dominated by narrow conceptualisations of security as 'freedom from threat'. Instead of framing matters of security solely through a lens of individual protection, we argue for a paradigm shift in the academic and political discourse of cybersecurity following differential and power-sensitive approaches. Based on a technofeminist analysis and different modes of critique confronting gendered cyber-insecurities, we draft the outlines of technoimaginaries based on feminist notions of vulnerability and care. The concept of digital care allows for a more holistic perspective on issues of security, and stresses the relevance of collective practices that aim towards being safe/r in hybrid offline-online environments.

Keywords: technofeminism, cybersecurity, digital care, technoimaginaries, vulnerability

INTRODUCTION

In the age of the cyborg—the co-existence and entanglement of cybernetic and organic forms of existence (Haraway, 1987)—the production of insecurity has expanded to our 'data bodies', our ways of communicating and organising online, our shared digital infrastructures and our computational machines. This is to say that the internet, in its commercialised and increasingly centralised form, is not safe, particularly for those affected by intersectional patterns of discrimination and oppression within the matrix of domination (Hill Collins, 2000). Gender-based violence, insecurity, and dependencies on centralised service providers characterise our participation in hybrid offline-online environments. The struggle to be safe has been taken up by techno-, cyber-, and transhack feminist initiatives and collectives who are working towards collective modes of empowerment and affective infrastructures of support and mutual growth. This struggle is fuelled by the belief that amid the ruins of capitalism (Lowenhaupt Tsing, 2017), another world and another technology can unfold, both more just and filled with care.

In taking up the question of being safe in the (cyber) spaces we inhabit, the following article contributes to technofeminist imaginaries as ways of speculating about safer futures that are grounded in an analysis of the material conditions of the production of insecurity, and committed to exploring radical alternatives alongside feminist strategies of repair and survival with technologies. Such technoimaginaries represent collective visions of desirable futures as well as providing a resistance against undesirable ones, shaped by shared conceptions regarding ways of living with digital technology (Jasanoff, 2015: 28; see also Toupin and Spideralex, 2018).

This article engages with cybersecurity as a field of practices, tools and discourses, investigating its potential for technofeminist adaptations. This includes not only the rejection or subversion of traditional forms of cybersecurity, but also the possibility of feminist appropriations and the development of alternatives based on the needs of women and trans and non-binary people.[1] The productive tension that guides this article is characterised by a

[1] Gendered discrimination affects a multiplicity of identities, including women, lesbians, inter, non-binary, trans, and agender persons. German-speaking feminists have coined the acronym FLINTA (with 'F' for 'Frauen', (English: 'women')) to comprise all these identities and avoid the exclusionary focus on 'women' or 'women*' as the subjects of feminism. However, while different terms highlight and include different aspects of gendered and marginalised lives, until the end of patriarchy, there

[1] *University of Münster*, GERMANY
[2] *Humboldt University*, GERMANY
***Corresponding Author:** wessalo2@uni-muenster.de

commitment to the strategic use of cybersecurity practices and tools for feminist self-defence, along with an insistence on the rejection of the traditional security paradigm that underlies the concept of cybersecurity.

Building upon recent feminist approaches to cybersecurity, the article aims to accompany activist endeavours for a safe/r internet with a theoretical investigation that sets out to formulate a feminist critique and technoimaginaries of overcoming cyber(in)security. Drawing on the rich history of feminist thought and recognising feminists' common fight against intersecting and correlating forms of oppression, our particular focus is the inherently gendered forms of and experiences around cyber(in)security.

According to established definitions (Bay, 2016; Slupska, 2019), cybersecurity is understood as a neutral set of methods that can be used in a value-free and objective manner, protecting computer systems and their users from digital dangers and attacks. However, in this article, we argue that the universalistic promise of cybersecurity often fails to address the safety needs of women and non-binary and trans people. Furthermore, we intend to demonstrate how, due to the underlying conceptualisations of liberal security, approaches to cybersecurity are entangled within the technopolitical production of insecurity that disproportionately affects marginalised groups. To challenge this status quo, we adopt a technofeminist perspective that centres the relationship between technology and gender, ultimately paving the way for alternative feminist, queer, and holistic approaches to safety with and alongside digital technologies. Our approach to technofeminism is informed by an intersectional lens, acknowledging the historically charged and interwoven manifestations of discrimination and power relations originating from and shaped by white supremacist capitalist patriarchy (Moore, 2016), with a specific focus on its technological implications.

Section 1 starts with an investigation of gendered cyber-insecurities that considers violence targeted against women and non-binary and trans people as well as gendered dependencies originating from the technopolitical composition of an increasingly commercialised and centralised internet. Section 2 examines the concept of cybersecurity as well as the intrinsic liberal notion of security, drawing on Melanie Brazell's (2021) distinction between positive and negative security. In Section 3, the article proceeds to bring together different strands of feminist modes of critique of cybersecurity, expanding on Daniel Loick's (2021) work to move towards a queer understanding of security. Finally, Section 4 delves into feminist technoimaginaries that go beyond the feminist adaptation of cybersecurity as a strategic means to counter patriarchal violence. In doing so, we aim to develop feminist technoimaginaries that can accompany efforts of feminist self-defence. Going beyond the negative conceptualisation of security, they emphasise the relational concepts of vulnerability and digital care.

In developing our argumentative thread, we draw on literature from the dominant discourse on cybersecurity as well as technofeminist engagements with theories and practices around cybersecurity and digital care (Amarela and Foz, 2022). Our theoretical reflections are inspired by intensive discussions with our communities, friends, teachers, and students, carefully crossing the lines of scholarly research and technofeminist activism.[2]

TECHNOREGIMES OF INSECURITY

Experiences of vulnerability, dependence, and abuse are not isolated incidents but follow intersecting patterns of discrimination that systematically devalue the lives of women and non-binary and trans people under patriarchy.

But how are gendered insecurities produced with regard to digital tools and infrastructures, and how does this inform strategies of self-defence and technoimaginaries of a safe/r internet? And finally, how does it play into the need to appropriate and/or subvert cybersecurity practices?

Following Isabell Lorey, who understands *precarisation* as a process that produces not only subjects but also "'insecurity" as the central preoccupation of the subject' (Foreword by Judith Butler in Lorey, 2015: viii), we define insecurities regarding gender as modes of destabilisation that are produced through neoliberal government and patriarchal forms of domination. Most practice-oriented feminist approaches to cybersecurity have focused on targeted cyber-insecurities mediated by digital infrastructures. Another approach, one often more theoretically informed, interrogates the gendered insecurity that stems from the technopolitical composition of digital infrastructures and the sphere of digital technology in and of itself. While both are ultimately intertwined, they have produced two different strands of discourse which, taken together, can generate a deeper understanding of the causes of gendered cyber-insecurities and are thus necessary for the development of a technofeminist critique of current technoregimes.

lies a responsibility to continually critically engage with the always incomplete and intricate act of naming as it is tied to cultural practices of exclusion/ inclusion, representation and remembrance.

[2] We are especially grateful for our enriching encounter with Mary Shnayien, our exchanges with Systerserver and the extended communities of TransHackFeminists, Cypher Sex, and Feminist Ninja, and our discussions with Vio and Foz from the Transfeminist Network of Digital Care. Our thanks go to the anonymous peer reviewers whose comments have substantially enriched this article as well as to the person who did the English proofreading.

The first take on matters of structural and gendered violence in online-offline environments is informed by feminist security studies and the field of human rights advocacy. It is centred around the notion of 'gender-based violence online'[3] (see edited volumes by Raghavan and Hussen, 2023; Powell et al., 2021; or Gentry et al., 2019). This form of violence consists mostly of targeted and often highly personal attacks, abuse, privacy violations, and forms of censorship directed against women and trans and non-binary people based on their assigned gender or gender presentation. Although often directed at individuals, this violence is sometimes specifically targeted against human rights defenders (Pavlona, 2021) and feminist collectives and organisations, including initiatives that fight for trans rights.

Gender-based violence online is conceptually framed in continuity with struggles that predate the emergence of the internet. It remains rooted in its status as primarily gender-based violence, with its connection to digital technologies as a secondary attribute. The framework of gender-based violence is crucial for formulating programs and strategies for a safe/r internet. Stressing the structural extent of targeted violence lies at the core of feminist modes of organisation and allows for strategic, solidary, and collective responses, cutting through the myth of 'lamentable single cases'. By assuming a structural stance, the framework also sheds light on how online violence that may not appear gendered can disproportionately affect those of us who have been brought up 'as girls', as we were structurally hindered from engaging with computer technology and often end up lacking access to resources and knowledge to protect ourselves (UNESCO, 2019). Furthermore, acknowledging online assaults as violence dismisses the trivialisation of seemingly virtual transgressions (Fairbairn, 2015: 244) by broadening the definition of violence beyond the physical.

However, online violence against women, non-binary and trans people cannot be separated from the ways in which it is mediated and enabled by digital infrastructures. While gender-based violence online is as old as the internet (Vickery, 2018), the virality of phenomena such as cyberstalking, cyberharrassment, doxing, and non-consensual sharing of pornographic pictures is linked to the rise of social media since the early 2000s and only began to receive scholarly and public attention in 2010 (Eikren and Ingram-Waters, 2016). Coinciding with the spread of social media, misogynistic hatred and anti-queer hostility on the internet have been increasing with the rise of alt-right movements and authoritarian regimes since the mid-2010s.[4] Furthermore, gender-based violence online has intensified due to the continued datafication of everyday life, which was intensified by the outbreak of the COVID-19 pandemic in 2020 (APC, 2020). While there are few studies available, feminist initiatives report an increase in digital assaults and a growing need for safety online (Spideralex, 2023), which corresponds to the recent emergence of feminist cybersecurity guides and other support infrastructures. Due to its focus on targeted violence as harmful or non-consensual acts by abusive actors, the framework of gender-based violence is less suited to focus on forms of discrimination which are structurally embedded in the technopolitical layers of digital infrastructures or manifested in platform governance. This is why the concept of gender-based violence must be combined with a technofeminist analysis of power relations inherent to the composition of today's centralised and commercial internet and the gendered sphere of (digital) technology.

Digital Dependencies

A second strand of discourse addressing the production of online insecurity stems from the interdisciplinary fields of media studies, studies of digital culture, and network or science and technology studies. It is often informed by a post-Marxist and Foucauldian analysis of neoliberalism and grounded in a critique of the processes of datafication and the concentration of power within monopolist corporations such as Google, Microsoft, Apple, and Amazon (van Dijck, 2014) that bring forth new ways of governance (Rouvroy, 2013). The influence of a few media platforms has expanded into almost every societal domain (education, finances, transportation, healthcare, reproductive and wage labour, activism, and so on). Surveillance, control, and the exploitation of humans and non-humans are inherent features of these platforms (Zuboff, 2019). However, the insecurities these platforms produce do not affect everyone equally. Instead, platform politics accompany and even amplify intersectional patterns of discrimination, such as sexism, ableism, racism, and classism (Apprich et al., 2018). Furthermore, while feminist analysis has investigated the manifold ways in which gendered differences are being produced online, we would like to point at two paradigms that shape the structural power imbalance at the core of the internet, disproportionally affecting women and non-binary and trans people.

The first one comprises the exclusion of women, queer, and trans people from technology-related spheres. This is not only true in terms of IT-related work environments but particularly in the development of Free/Libre and

[3] Similar terms are technology-facilitated-gender-based violence, violence enabled by ICT, online/digital gender (based) violence, cyber violence against women, online misogyny, and online violence against women. See Spideralex (2023) and Raghavan and Hussen (2023).

[4] The relation between the rise of social media and personalised advertising and the rise of alt-right movements is another topic of interest.

Open-Source Software (e.g., Robles et al., 2016; Eghbal, 2016) and in the hacker scene (Coleman, 2013).[5] The monopoly over technical and especially computer-related fields by cis men is a crucial factor contributing to gendered digital insecurity (Cockburn, 1988: 8). A significant portion of the digital infrastructures used daily by women and trans and non-binary individuals and collectives is developed, established, and maintained by cis men, fostering dependency relationships and gender-specific vulnerabilities (Wajcman, 2004: 20). Although multifaceted factors contribute to the exclusion of women and non-binary and trans people from technology-related spheres, technofeminists like Judy Wajcman consider the culturally encoded gendering of technologies to be the root of the problem. This, in turn, stems from the division of labour into productive (high-tech related) work and reproductive (low-tech related) work, which is decisive for the binary conception and devaluation of femininity (Wajcman, 2004).

The second paradigm that shapes technoregimes of insecurities addresses the production of disempowered user subjects. With the ongoing centralisation of the internet, the increased use of web technologies, computers, and smartphones has been characterised by an intensified user/service paradigm (cf. Kleiner, 2010). It describes a power imbalance between users and commercial providers of digital services (mostly owned and led by white cis men), in which 'terms of use' are not only enforced through legal means but also the design and functionality of the platforms. The opaqueness and complexity of technological infrastructures and the push towards cloud computing (that is, the concentration of computational power away from local machines into remote data centres) further drives the technological disempowerment of users who systematically lack the privileges and knowledge to access or understand their functionality, beyond prescribed, basic modes of media consumption and content production (Suárez-Gonzalo, 2019: 176). In this way, limited technical expertise and the lack of alternatives keep user subjects dependent on the infrastructures of extractive, profit-oriented service providers, which not only exposes them to misogynistic platform governance but also lays the foundation for the exploitation of personal data within the current extractivist platform economy (Srnicek, 2017).

Digital mediated violence and the gender-specific vulnerabilities of women and non-binary and trans people are multifaceted and structural problems whose causes lie in the entanglement of patriarchy, platform/techno-capitalism, and national (digital) policies. While the situation of violence differs in various cultural and national contexts, practices of violence have become global through (nearly) globalised online communications. Within this framework, forms of structural violence and insecurity are dependent on cultural and political factors and are influenced by national legislation as well as the specific conditions of use of digital technologies and platforms. Having investigated the structural causes of the dependencies as well as the violence and harassment that women and non-binary and trans people are facing online, the necessity to find and discuss ways of being safe/r becomes clear. One dominant concept in the discourse around safety online is cybersecurity.

CYBERSECURITY AND ITS FEMINIST CRITIQUE

Common definitions frame cybersecurity as a 'set of protocols, technologies, and practices designed to protect against threats mediated by digital technology' (Slupska, 2019: 84). To defend against, mitigate, or even overcome cyber-insecurities, feminists and other activists have long relied on the adaptation of cybersecurity practices to stay safe online. Cybersecurity practices such as encrypted communication, password management, profile anonymisation, and the use of privacy-preserving and Free and Open-Source tools are an integral part of keeping women and trans and non-binary people safe online. But what are the implications behind the conception of cybersecurity and its common depiction as a neutral toolbox to be used for all kinds of purposes, including feminist ones? And what does the notion of security tied to cybersecurity practices mean for the possibilities and limitations of feminist adaptions?

Liberal Conceptions of Cybersecurity

Among increasingly popular and overlapping terms such as digital-, IT-, computer-, information-, and data security, cybersecurity remains the most frequent framework used in academic discourse throughout the last decade (Veale and Brown, 2020: 1). While each of these terms sets a different and sometimes more narrow or technical focus, we speak of cybersecurity explicitly to highlight the spatial metaphor that informs our understanding of the internet and communication technology. Cybersecurity takes its prefix 'cyber' from the concept of 'cyberspace', an idea which goes back to William Gibson's fictional story *Neuromancer* (Veale and Brown, 2020; Bay, 2016: 5). This term conceptualises space 'as a time-dependent set of interconnected information systems and the humans that

[5] The project Lelacoders by the Catalan Donestech Initiative documents women, lesbians, intersex, non-binary, trans, and agender individuals involved in the development of free software, hacking, and cyberfeminism. It aims to counter the invisibility of (missing) role models. For more information about this project, please visit: https://donestech.net/. (Accessed 18 July 2023).

interact with these systems' (Lorents and Ottis, 2010: 1, cited in Bay, 2016: 5; for a detailed reflection of the term cyberspace, see Bay, 2016: 5ff.).

The multiplicity of approaches to cybersecurity makes it challenging to undertake critical analysis and establish clear classifications (Hansen and Nissenbaum, 2009; Schatz et al., 2017; Bay, 2016). However, while the objects of cybersecurity may differ (computer systems, users, data, national integrity, economic relations and markets, critical infrastructure), there remain two things common to most, if not all definitions of cybersecurity. The first is the understanding that security aims at and describes something (a system, a technology, a process, etc.) that is free from threat (Craigen et al., 2014: 14). The second point is that this freedom from threat is a condition which is practically impossible to achieve, and that it is often a time-critical battle of resources between those who protect and those who attack (Shnayien, 2022: 48). This agile conception makes cybersecurity a framework which can strategically adapt to all kinds of environments and attack scenarios, often defined within so-called *threat modelling*. Yet despite its seemingly value-free applicability, the prevailing notion of cybersecurity is as a negative and paranoid conception of security that we will further explore in the following section.

Negative security is tied to the condition of threat and is characterised as security *from* (Brazell, 2021; Loick, 2021). The precedent condition of threat that needs to be defended against is what characterises security as an inherently paranoid mindset: to achieve security, we must operate under the assumption of the worst circumstances.[6] In the realm of cybersecurity, this is exemplified by the mimetic practice of 'pentesting' or 'penetration testing', which consists of an authorised attack against a system or a company to identify so-called 'vulnerabilities' in order to protect against malicious attacks in the future (Petty, 2016: 82). The violent language that maps 'attacker' and 'victim' onto a binary and gendered script is not incidental, as security is inherently tied to the epistemic and often violent act of drawing a border between those in need of protection and those that constitute the threat (Laufenberg and Thompson, 2021).

This goes back to a liberal conceptualisation of security, which is linked to the ideal of individual freedom and primarily established through the right to property (Loick, 2021: 270). Based on the anti-social liberal idea of society as nothing more than the sum of isolated individuals, security becomes a guiding principle for the reproduction and solidification of the capitalist world order (Laufenberg and Thompson, 2021). This concept of security is crucially linked to the construction of an 'external threat' that legitimises the existence of the state's monopoly on the use of force and its security apparatuses. Current critical interpretations of this negative security paradigm point out that the construction of a threatening 'outsider' often relies on racist ideologies and strategies of 'othering' (Loick, 2021: 271).[7] Moreover, it is entangled in patriarchal logics that justify military and police security apparatuses through the postulated essential vulnerability of women and other marginalised groups (Brazell, 2017).

However, the liberal conception of security extends beyond its implications for a national security paradigm and state-led protection of citizens or even the free market and has been claimed by libertarians to empower the individual over the state. This is evident in the history of digital cryptography, which serves as a fundamental underpinning of the technical aspects of cybersecurity (Shnayien, 2022). The liberal value of cryptography as a means to protect the individual's liberty from the state was the central interest of the cypherpunks – a libertarian community of privacy advocates that fought against the government regulation of cryptography in the 1980s and 1990s. Their impact has undeniably shaped transformative digital activism and informed initiatives such as Tor and WikiLeaks. However, the unrealised aspirations of a crypto-anarchist global structure serve as a valuable lesson, illustrating that cryptography, despite its potential to challenge concentrations of authority, can also inadvertently reproduce them (Shnayien, 2022). This is not to say that cryptography is a neutral tool. As we have demonstrated, the foundational concept of liberal and negative security carries both ideological and epistemological implications, whether it is employed to safeguard the nation or the individual or to provide means of (feminist) self-defence. Rather, it encourages us to consider alternatives that are attuned to power dynamics and collective values – approaches to achieving safety that extend beyond the binary framework of 'self' and 'other'. This exploration will be continued in the next section.

Feminist Critique(s) of Cybersecurity

On a theoretical level, feminist engagements with cybersecurity are rooted in many different fields of analysis, including feminist traditions of self-defence and digital activism as well as theories of (in)security, computer technology, and gender. Among these, it especially draws from cyber- and technofeminist explorations of the

[6] In her text 'Paranoid Reading and Reparative Reading', Eve Kosowsky Sedgwick (2003) has demonstrated how paranoia is deeply tied to the production of paranoid knowledge and is therefore a fundamentally epistemic manoeuvre based on the need to know ('There must be no bad surprises', Sedgwick, 2003: 130) to defend or protect against. Subsequently, security (knowledge) is a way to know the world which does not allow for any alternative (more positive) interpretations as those would compromise the strong assumptions of ubiquitous threat on which it is based.

[7] Mary Shnayien further shows that this kind of border work is based on an immunological discourse that separates 'self' from 'other' (Shnayien, 2022: 127).

gender–technology relationship dating back to the 1980s (including Haraway, 1987; Wajcman, 2004; Fernandez and Wilding, 2002). As we will demonstrate, this concept also connects with the analysis of power dynamics in security frameworks, encompassing discussions of police and military entities, and of the dominant power structures within the state (Gentry et al., 2019; Laufenberg and Thompson, 2021). Additionally, it corresponds with the criticisms directed at neoliberal regimes of precarity (Lorey, 2015). Given the scope of literature and the focus on different aspects of the gendered production of cyber-insecurities, feminist approaches can be roughly characterised according to one or two main lines of critique.

The first mode of critique is motivated by the possibilities of feminist adaptations of cybersecurity practices and resources. This critical approach to cybersecurity highlights matters of accessibility and usability, stressing heterogeneous security needs, and is more often expressed in practice-based materials such as guides, handbooks or policy reports. Nonetheless, James Pierce, Sarah Fox, Nick Merrill, and Richmond Wong (2018) suggested the concept of 'differential vulnerabilities' as a theoretical foundation resulting from their analysis of cybersecurity toolkits. The concept describes the different and structurally determined security needs of marginalised groups and considers the emergence of methods of self-defence and community-based strategies as a symptom of failing institutions and companies with their generalised claims of securitisation. The central point of criticism in this mode of critique is the idea of 'normalised' security needs. This entails examining the digital privileges and overall (financial) capacities of the 'typical user' of a cybersecurity product or resource and acknowledging the difficulties that arise when extending cybersecurity measures to individuals who do not align with these privileged norms and exclusive standards.

The inadequacy of mainstream and male-dominated cybersecurity (both as a product and as a wider field of expertise) is especially evident in the ways one can acquire knowledge about it: many tutorials are difficult to access without particular (language) skills or online search strategies, and they are generally made for users with advanced technical knowledge and cutting-edge hardware and software, often neglecting older versions or setups (Foz and Vio in Lange and wessalowski, 2023). Furthermore, help forums for technical matters are often characterised by toxic language ('Read the Fucking Manual') and an obligation to have prior knowledge, which can lead to further exclusion (Reagle, 2014). Finally, learning about cybersecurity is a laborious, time-intensive, and often prevention-oriented undertaking, which makes it less likely to be taken on due to (time) precarity, (gendered) care commitments, and wage labour relations.

Thus, feminist and intersectional critiques of the accessibility and usability of cybersecurity and digital self-defence have been crucial in addressing inequalities and fostering hands-on approaches to develop cybersecurity material for more diverse users and use case groups. However, this mode of critique runs the risk of remaining within a purely diversifying logic of inclusion that can easily be adopted by companies thereby fostering new and diversified dependencies to centralised service providers (closing some of the gendered insecurity gaps while widening others). To avoid the dilution of its critical potential, it therefore needs to be combined with a thorough analysis of the scope of gendered cyber-insecurities. This critique should also encompass the technical necessity of implementing security measures and the linked negative interpretation of security (Strohmayer et al., 2022) and will be further developed in the following section.

In contrast to the negative notion of liberal security that emphasises freedom from threats, feminist as well as other power-sensitive and intersectional approaches propose a shift towards positive conceptualisations of security as 'security to', 'holistic security' or even 'safety' (Petty, 2016; Loick, 2021; Binder and Haché, 2023). These perspectives criticise individualising and technocentric framings of security which do not account for how the production of insecurity is tied to structural patterns of discrimination. As a first step towards feminist technoimaginaries, positive notions of security are rooted in the interdependent and communal development of relationships and collective agency (Petty, 2016: 83; Loick, 2021: 267). Daniel Loick identifies how positive notions of security resist the foundational logic of negative conceptualisations (Loick, 2021), which are also found and expended in feminist and other power-sensitive inquiries of cybersecurity. One differentiation addresses the claim of universal securitisation which according to Loick misses the 'differential character of security production,' (Loick, 2021: 273, translated by the authors). Due to the binary logic of threat modelling ('self vs other'), negative notions of security categorically omit the selective quality of security production ('security for some'). Presupposing a morally infused idea of what needs to be protected (the 'home', 'women and children' or 'national integrity'), the universal claim of securitisation is crucial in obfuscating the costs of security as it prevents an interrogation of the violent drawing of (national) borders separating those in need of protection from those labelled as threats.[8] On the contrary, positive notions of security take into account the intricacies of producing security 'for someone', which can be traced back to feminist epistemologies that privilege situated, as well as materially and bodily

[8] In her text 'Safety vs Security: Are You Safe or Are You Secure?', Tawana Petty shows how the implementation of security systems such as security cameras can constitute a threatening scenario for marginalised individuals, including undocumented immigrants, Black individuals, those affected by gender-based violence, or other marginalised groups (Petty, 2016: 82) in order to propose a differentiation between technocentric security and more holistic understandings of safety.

grounded, standpoints (Harding, 2004). Feminists thus oppose the universal claim of cybersecurity with an understanding of security as something that is always partial, site-specific, context-dependent, and historically tied to the structural enforcement and changing regimes of unequally distributed uncertainties and insecurities (Hansen and Nissenbaum, 2009: 1172).

Another recurring focus of feminist criticism of security concepts is the division between a security-relevant public sphere and a devalued private sphere that systematically excludes structural partner violence and sexualised violence (Radloff, 2013; Slupska, 2019). Daniel Loick describes this as a second differentiation movement towards a positive understanding of security, challenging the domination of public discourse by certain topics, such as migration, terrorist threats, and crime, while others such as ecological and social security receive little public attention and are often not even framed as security issues. The devaluation of seemingly private threats and the associated violence is also evident in the juxtaposition of informational privacy as a social concern and security as a technical matter (Dourish and Anderson, 2006). Resistance is expressed through the adaptation of the traditional feminist credo, 'The personal is political!', as a militant call for the digital space: 'Private data is political!' (Suárez-Gonzalo, 2019). However, arguments advocating for the prioritisation and acknowledgement of issues like gender-based violence face the potential of falling into the same inclusionary logic that characterises diversification strategies. This is evident, for example, in cases where feminist critique appeals to the legal framework for cybercrime or to the police. While reformist approaches on the one hand, find that security forces do not take gender-based violence online seriously enough and call for raised awareness, diversification of measures, or adaptation of relevant laws, abolitionist approaches on the other hand, focus their critical examination on the monopolies of violence held by states and powerful actors such as tech companies.[9]

Feminist critiques of cybersecurity also highlight the dangers of dominant technology-centric approaches. Researchers such as Tawana Petty (2016) and Julia Slupska (2019) position themselves against a narrow understanding of security that focuses on technical damage or compromising of computer systems rather than social impacts. Since threats and dangers can only be understood in the context of the analogue/digital hybridity of contemporary life, cybersecurity must accordingly be perceived as a techno-social practice (see Dourish and Anderson, 2006). The underlying critique of techno-solutionism, which refers to looking for technical fixes to more-than-technical problems, is sometimes expressed as a shift away from 'measurable' security and towards holistic notions of safety as a relational process of *being-with*. Tawana Petty touches upon this concern in her thoughtful distinction between matters of 'safety' and 'security' when she states that although security mechanisms can provide us with a measure of comfort, 'there is no magic spell that can guarantee our safety' (Petty, 2016: 82). The idea of safety as a process of *being-with* thus acknowledges uncontrollable risk as a central aspect of human life in a world shaped by complex and intersectional ecologies of humans, technology, and non-human actors.

Another perspective aiming for a positive understanding of cybersecurity revolves around the concept of safe/r spaces.[10] Starting as physical gathering sites, the feminist implementation of safe/r spaces dates back to the efforts of separatist women as well as women, lesbian, and trans groups during the height of second-wave feminism in the 1970s and 1980s (Clark-Parson, 2018). These spaces have continued in a separatist tradition, addressing the constant exposure to hegemonic culture and patriarchal violence by centring the needs of marginalised people and intersecting identities related to gender, sexual orientation, ethnicity, or dis/ability. In feminist contexts, safe/r spaces often gather people who do not identify as cis men to foster modes of mutual support, feminist organisation, and transfer of critical knowledge and strategies of resistance. Building on the spatial metaphor of cyberspace as a space to be inhabited by women and non-binary and trans people, the concept of safe/r spaces has been expanded to and interwoven with online infrastructures such as websites or chat groups. Just like their offline equivalents, safe/r spaces that are (primarily) set in online environments are constantly involved in a processual reflection on power relations, ultimately striving to create an interim environment free from patriarchal violence and discrimination. However, while these spaces have been shown to have the potential to resist against neoliberal precarisation tendencies, the incorporation of and proximity to negative definitions of security as 'freedom from' can sometimes lead to the reproduction of a 'techno-security culture' (Kämpf, 2014: 71). Additionally, safe/r spaces online are often built on commercial social media platforms that restrict certain use cases and security needs, such as encryption or anonymity, by default.

[9] While the extend and the subjects of the violence conducted by states differ depending on their governments, abolitionist approaches develop a fundamental critique of border regimes as well as the institutionalisation of prison and police forces which are constitutive to the manifestation of modern nation states (Brazell, 2017).

[10] Within activist circles, designated 'safe spaces' are criticised due to the presumed promise of safety ('Safe for whom?'), which has led to an increasing discourse on 'safer spaces'. The shift towards a more relational and less factual expression presupposes that due to complex and intersecting forms of marginalisation, it cannot be assumed that a space is truly safe for everyone. Furthermore, the concept of safe/r spaces has given rise to debates around affirming/deconstructing identarian logics and identity politics as well as to the means and the enforcement of 'separation'. The concept has also been instrumentalised against vulnerable groups, such as in the case of trans-exclusionary hate groups.

Nonetheless, reclaiming commercial social media is a common strategy among diverse feminist groups to utilise networking opportunities, ensure visibility, create spaces for participation, and facilitate the exchange of experiences or knowledge resources. Within these strategic approaches, the inherent politics surrounding the insecurity of commercial platforms, with their exploitative business models that result in disempowered user subjects, and usage conditions aligned with cis male norms (such as 'nipple censorship') are often problematised and reflected upon (Clark-Parson, 2018). Thus, the relationship between feminist initiatives and commercial social media has always been ambivalent, with a growing desire for self-governed and non-exploitative alternatives.[11]

In conclusion, both lines of feminist critique on cybersecurity unveil distinct aspects of the gendered insecurities embedded within digital spaces. Both strengths illustrate the breadth of feminist engagements with cybersecurity and the multifaceted reasons for and effects of online insecurity. As a critical reflection on the specific configurations of power relations in the hybrid offline-online space, they convey different strategies of subversion and over-affirmation, ranging from reformist to abolitionist approaches. This signifies a departure from the insecure user subject toward an empowered, self-determined collective and feminist subjectivity that not only adapts existing cybersecurity practices but furthers the creation of self-governed infrastructures catering a communal and locally developed sense of security.

VULNERABILITY AND CARE AS TECHNOFEMINIST IMAGINARIES

As a first step towards technofeminist imaginaries of being safe around digital technologies, notions of positive security provide an alternative to the constitutive relationship between state and citizen (Zaharijević, 2013: 71), which is inscribed in liberal conceptualisations of security as 'freedom from threat.' Contrasting the individualising precept of capitalist world order, these positive conceptions are social and ecological in that 'the other' is not primarily seen as a threat (or as 'threatening' competition) but as the relational aspect of co-existence and collective agency (Loick, 2021: 275). At its core lies the notion that security is not pursued through protection and isolation, but rather is achieved through 'individual and collective self-determination' (Loick, 2021: 277, our translation).[12] This begs the question: how and to what extent can positive security and feminist notions of safety be extended into the realm of cyberspace? To address this question, a re-evaluation of our perception of cyber-insecurities in relation to vulnerabilities becomes necessary. Additionally, we set out to explore the analogies between queer sexuality and interactions with cyberspace, as discussed by Daniel Loick and Mary Shnayien in their exploration of queer interpretations of (cyber)security.

Drawing on the theories and collective works of Judith Butler and Isabel Lorey, queer interrogations of security have guided us towards recognising vulnerability as an intrinsic aspect of all bodies in the face of prevailing power dynamics (Butler, 2006; Butler et al., 2016). Vulnerability serves as a framework to deconstruct the neoliberal tales of self-sufficiency and independence that follow the gendered presumption that 'in the beginning, apparently, there is a man, and he is an adult and he is on his own, self-sufficient' (Butler, 2020: 36). It challenges the idea of (male) immunity to threats and, therefore, the (male) gesture of denying an existential need for safety or care. Vulnerability is understood as a relational quality through which and in which we are exposed and that unavoidably points to different modes of dependency, whether on others or on more-than-human, social, material, or digital infrastructures (Butler, 2020: 41).[13] This also means that with conflicts being a potential part of every social bond, their destructive force becomes an inevitable aspect of any relation based in vulnerability (Butler, 2020: 39).

Ontological vulnerability, which is followed up in Lorey's take on 'precariousness' (Lorey, 2015), must be understood as a driving force behind liberal security regimes in the sense that it is not only politically produced but also distributed by and through unequal mechanisms of power (Butler et al., 2016: 5). This results in the redistribution of security along the lines of intersecting patterns of discrimination. Lorey similarly differentiates between precariousness and precarity, marking that 'precarity denotes the striation and distribution of precariousness in relations of inequality, the hierarchization of being-with that accompanies the processes of othering' (Lorey, 2015: 12). Likewise, vulnerability should not only be perceived as ontological but as an unevenly distributed relation, a focal point of critique within the realm of cybersecurity.

[11] Projects such as feminist servers that provide and self-host their own digital tools such as wikis, etherpads, or code repositories have combined the idea of safe/r spaces with an emancipatory approach to building and federating their own decentralised infrastructures (Lange and wessalowski, 2023).

[12] Loick names transformative justice initiatives as well as abolitionist approaches fighting against the carceral system as examples that work towards the realisation of positive security engaging with and producing forms of community (Loick, 2021: 274).

[13] Perceiving the human body as inherently dependent on some form of infrastructure (broadly understood as environment, social relations, technology, etc.) implies a notion of vulnerability that fundamentally challenges the dominant ontological understanding of the subject (Butler, 2020: 21).

This is where the analogy of queer sexuality and digital practices of networking with computers comes into play. As Mary Shnayien shows, metaphors around safer online practices, sometimes called 'safe hex', are significantly influenced by the medical vocabulary that dominated the discourse around the HIV/AIDS pandemic, which overlapped with the first appearance of so-called 'computer viruses' and worms in the 1980s. 'The programme of "personal systems hygiene" meant an extension of one's own body hygiene to one's own machines, in order to protect both bodies as *self* from all forms of biological and informatical *other*' (Shnayien, 2022: 136, translated by the authors). Shnayien warns against the adaption of a liberal logic of personal responsibility, derived from negative security. This highlights the necessity of both 'safe sex' and 'safe hex', as approaches centred on personal responsibility have been misused to further stigmatise marginalised groups for their supposedly risky behaviour and lack of prevention. In contrast, Daniel Loick follows a more positively connotated interpretation, asserting that by acknowledging and embracing risks amidst precarity, queer sexuality has not only embraced transformative strategies to address vulnerabilities but has also engendered practices and insights about safer sex that challenge the assumption of 'normal' (and therefore seemingly risk-free) sexuality (Loick, 2021: 281).[14] Consequently, it has been argued that rather than stemming from the unrealistic appeal to abstinence from risky behaviour, security is only achieved through actively negotiating and prioritising safety while recognising insecurity in all forms of expression and encounters, not just marginalised ones. 'The impossibility of security is at the same time the condition of its possibility' (Loick, 2021: 280, translated by the authors). This interpretation of security diverges from an idealised state of complete safety by instead taking the affirmation and knowledge of insecurity and risk as its starting point.

As a technosocial space constituted by connecting machines and the cyborg inhabitants of digital infrastructures, cyberspace is inherently promiscuous and vulnerable. While this insight might at first seem similar to the paranoid approach and even the language of cybersecurity (managing 'vulnerabilities' before they can be 'exploited'), the focus of positive cybersecurity is on fostering the technosocial connections that we want to foster and knowing and having strategies for dealing with the risks involved. Queering cybersecurity is thus a matter of problematising normalised behaviour within an economy of security that leads to the stigmatisation of promiscuous and 'risky' behaviour outside the seemingly secured walled gardens of commercial platforms and the black-boxed products of giant tech companies.

Queer and feminist viewpoints encourage us to reframe vulnerabilities not as shortcomings but as an ontological condition of life and co-existence – a condition that enables relations of connection and empathy. This appreciation of vulnerability is based upon the importance of individual and collective self-determination and the possibility of informed and consensual decision-making regarding dependencies within the pervasive technological complexities of our present (Butler et al., 2016: 13).

Given our analysis of the intersectional insecurities experienced by women and trans and non-binary people, we argue for a perspective on security that centres around vulnerability and care as a starting point towards being safer online. The turn from security to care as an imaginary aimed towards alternative security practices is supported by etymological tracing of the English term 'security' from the Latin noun '*securitas*'. Removing the prefix 'se-' ('without') leaves its root, the Latin word '*cura*', which means 'care' or 'worry'. Security translates literally to a state of 'freedom from worry' or 'carelessness' (Folkers and Langenohl, 2020: 1) unveiling how the negative conceptualisation of security is indeed rooted within the word itself. Drawing on historical entanglement with gendered reproductive work (Tronto and Fisher, 1990), the notion of care has for a long time been the focus of feminist debates and discussion. While we follow Marxist critiques by scholars like Silvia Federici (2019) that pointed out that the capitalist separation between productive and reproductive work has led to the devaluation of care and its practices, we emphasise an understanding of care as a transformative framework and a starting point for feminist inquiries and interventions. Here, we draw on works by science and technology scholar Maria Puig de la Bellacasa (2017) who has argued for an ethos of care that challenges traditional notions of ethics and knowledge. Engaging with a broad notion of care by Joan Tronto and Beatrice Fisher (1990: 40), we understand care as 'everything that we do to maintain, continue and repair "our world" so that we can live in it as well as possible. That world includes our bodies, ourselves, and our environment, all that we seek to interweave in a complex, life sustaining web' (Tronto and Fisher, 1990: 40).

Bellacasa highlights the importance of going beyond anthropocentric perspectives in acknowledging the interconnectedness of humans with non-human entities and the environment. This leads to an understanding of care that involves recognising relationships, emotions, and technologies as fundamental to the ways in which we perceive the world. In this context, care becomes more than just an ethical approach to doing something, instead evolving into a transformative way of existence (de la Bellacasa, 2011: 100). Directing attention towards a

[14] A similar argument which has been productively applied to digital practices can be found in the feminist principle of consent (Peña and Varon, 2019). Giving and asking for consent reverses the assumption of having to decline seemingly 'normal' interactions or sexual practice – an assumption that is based on a negative notion of security – into a shared responsibility to express agreement to engage with each other on our own terms.

technopolitical interpretation of care that critiques the prevalence of technoscientific rationality and advocates for an embodied and context-sensitive approach to knowledge (Lange and wessalowski, 2023) leads us to ask: How can notions of care support the process of reshaping the future of cybersecurity beyond its present framework?

Viewing security through the lens of care can highlight the need for protective care that goes beyond the dangerous idea of 'liberal forms of individualism' (Butler et al., 2016: 3) or the prioritisation of military protection of nations (Folkers and Langenohl, 2020: 3). This inherent fusion of security and care implies a spectrum of securing and safeguarding practices that diverge from the conventional state-centric or even individualist paradigms. However, it is crucial to acknowledge that the concept of 'caring security' does not promise a simplistic comprehension of security. Instead, it is an attempt to unveil pronounced dependencies and hierarchies (Folkers and Langenohl, 2020: 11). Therefore, our understanding of care is closely linked to what Butler calls 'aggressive nonviolence', meaning a condition 'that emerges amid conflict, one that takes hold in the force field of violence itself' (Butler, 2020: 40). Butler contends that nonviolence is not merely a reaction stemming from aggressive emotions such as anger or rage; rather, she conceptualises it as a practice that must be aggressively pursued (Butler, 2020: 21). In that sense, aggressive nonviolence' is not to be thought of as a contradiction, but rather as a starting point for action. This is the same stream of thought we follow within our critique of the dominant cybersecurity paradigm by acknowledging inevitable vulnerabilities.

The French philosopher Elsa Dorlin draws on a similar notion with her term 'dirty care', which refers to a caring practice of self-defence that people are forced to use as an instrument of resistance when violence is an inherent part of their everyday lives (Dorlin, 2022). Dorlin highlights that while feminist theory tends to characterise care as an ethical stance defined by compassion, love, and empathy, a different form of care arises from enduring violence. This 'dirty care' for others goes beyond nurturing—it is driven by the need to protect ourselves from potential harm. Within this notion of care as a practice of self-defence, Dorlin points out that only some selves are regarded as entitled to self-defence (Dorlin, 2022: 41ff.). Thus, her concept not only broadens the discussion by directing attention to the representation of essential social ties and the unequal ways in which the selves worth defending are articulated within a political field (Butler, 2020: 16), but it also leads us to reformulate our understanding of security, especially in the face of increasing violence and insecurities.

Additionally, the notion of 'dirty' care stands in contrast to the neoliberal appeal to resilience. According to Sarah Bracke, in periods of uncertainty within the liberal security paradigm, resilience emerges as an updated concept of security (Bracke, 2016: 57). The concept serves as a recalibration of security, aligning with conventional preventative and defensive measures but emphasising an understanding of security as 'minimizing impact and erasing traces' (57), fostering the ideal of 'preparedness' (63) in the face of precarious circumstances. Its core components, flexibility and elasticity (65), further draw on gendered dimensions and racial politics that cultivate the idea of a resilient subject as one 'who can absorb the impact of austerity measures and continue to be productive' (61).

In contrast to the prevailing neoliberal paradigm, this article advocates for an implementation of safety that negates the necessity for resilience, allowing one to embrace vulnerability as a strategic form of resistance (Butler et al., 2016). While resilience underscores the importance of individuals adapting to given situations, particularly in the context of violence and crisis, resistance emphasises the imperative to reject prevailing conditions and endeavour to transform situations, processes, and practices. This approach holds the promise of cultivating new forms of collective agency that not only acknowledge vulnerability as a valuable resource but also claim equality, freedom, and justice as their political objectives (Butler et al., 2016: 7).

In that sense, transposing the framework of care to the domain of cybersecurity challenges the prevalent antagonistic approaches that characterise the field. An ethos centred on care compels us to focus on the well-being and safety of individuals and communities and overcomes the exclusive focus on technical defence mechanisms. This shift requires a re-evaluation of security strategies to ensure they reflect human experiences and vulnerabilities. Hence, recognising vulnerabilities not as mere shortcomings but as integral aspects of co-existence can empower the cultivation of more compassionate and sustainable strategies for being safe online in the form of self-empowerment, collective agency, and protection (Butler et al., 2016: 2).

Following Sheila Jasanoff's 'sociotechnical imaginaries' framework and concept, technological advancements are shaped not only by scientific knowledge but also by societal visions of 'desirable futures' (Jasanoff, 2015: 13). These collective imaginaries influence policy decisions, regulatory frameworks, and ethical considerations surrounding technology. Drawing inspiration from the comprehensive efforts of Brazilian activists, we aim to approach cybersecurity through the lens of 'digital care' (Amarela and Foz, 2022; Zakharova and Jarke, 2024). This approach seeks to overhaul the militarised and capitalist narratives and methodologies inherent in traditional notions of negative security and reframe them within the context of safety nurtured through digital care. Thus, at the core of our technofeminist critique of cybersecurity lies an ethics of care, which accentuates interconnectedness as relationality, empathy, and the (responsible) ethical obligations within more-than-technical relationships. A care-centred feminist critique of cybersecurity redefines and broadens the prevalent concept of cybersecurity by

challenging its biases and mechanisms of exclusion, thereby transcending its limitations. By combining care ethics and intersectional viewpoints, we can progress towards a cybersecurity paradigm that prioritises relational as well as holistic approaches to safety, rather than advocating for the predominant, anti-social vision of security as 'carelessness' to be achieved by technical fixes.

CONCLUSION

There is a compelling need for a paradigm shift in the academic and political discourse on cybersecurity. This shift involves transforming the prevailing negative and paranoid perception of cybersecurity as 'freedom from threat', which is tied to the epistemological act of 'othering', and its entanglement in the gendered and intersectional production of cyber-insecurities. Drawing on different strands of (techno)feminist critique, we argued that liberal concepts of cybersecurity based on an individualised idea of society and rooted in the discourse around national security ultimately fail to provide safety, especially for women and trans and non-binary people in online-offline environments. The collective work towards technofeminist imaginaries must instead be based upon an analysis of the causes of gendered cyber-insecurities. It must also consider both targeted violence online as well as technopolitical dependencies in the extension of the (physical) domination over women and non-binary and trans people under patriarchy, which today manifests within the centralised and commercialised internet.

While acknowledging the fight against further precarisation and the work of making cybersecurity practices more accessible, we have further explored technofeminist imaginaries based on positive conceptualisations of security and the feminist notions of care and vulnerability. These are rooted in the recognition of vulnerabilities as a precondition for more-than-human connectivity. It emphasises the essential role of an empowered subject who knows about the unequal power dynamics that emerge from within current digital environments. A careful approach to being safe online must be paired with strategies and competencies concerning not only the care and protection of one's machines, data, and infrastructures but also the care and protection of others navigating the technosocial spaces of the digital technologies we engage with.

Nevertheless, imaginaries exist within online–offline environments that cultivate safer spaces where women and trans and non-binary people share experiences, gain knowledge about (in)securities, and learn about practices of digital care. In this context, the distinctiveness of technofeminist imaginaries of digital care is obvious. Its visions are grounded in an alternative concept of security—one that strives for collaborative practices and empowerment rather than individualistic defence-oriented strategies based on liberal cybersecurity concepts. Consequently, technofeminist imaginaries based on care not only introduce alternative perspectives on user identities and diverse methods of securing oneself, others, technologies, and various forms of techno-human connection, but they also embody a set of different norms that underpin these visions. Following the trace of these norms can pave the way towards more just and safer futures. This journey toward safety departs from prevailing paradigms of cybersecurity and embraces alternative conceptions of vulnerability, care, and technosocial connections that resonate with the ideas and critical thought of technofeminism.

REFERENCES

Amarela and Foz. (2022). Digital care and philanthropy: Findings and basic recommendations, *FASE*. Available at: https://fase.org.br/wp-content/uploads/2022/10/Digital-care-and-philanthropy.pdf. (Accessed 1 September 2023).

APC (Association for Progressive Communications). (2020). COVID-19 and the increase of domestic violence against women: A submission from the association for progressive communications to the United Nations special rapporteur on 'violence against women, its causes and consequences', *Association for Progressive Communications (APC)*. Available at: https://genderit.org/sites/default/files/apc-062020-srvaw-covid19-domesticviolence.pdf. (Accessed 1 September 2023).

Apprich, C., Cramer, F., Hui, W., Chun, K. and Steyerl, N. (2018). *Pattern Discrimination*. Lüneburg, Germany: Meson Press. https://doi.org/10.14619/1457

Bay, M. (2016). What is cybersecurity? In search of an encompassing definition for the post-Snowden era. *French Journal for Media Research*, 6(28), 1–28.

Bellacasa, M. P. de la. (2011). Matters of care in technoscience: Assembling neglected things. *Social Studies of Science* 41(1), 85–106. https://doi.org/10.1177/0306312710380301

Bellacasa, M. P. de la. (2017). *Matters of Care*. Minneapolis, MN: University of Minnesota Press.

Binder, I. and Haché, A. (2023). A feminist conversation on cybersecurity. Available at: https://genderit.org/editorial/feminist-conversation-cybersecurity. (Accessed 1 September 2023).

Bracke, S. (2016). Bouncing back: Vulnerability and resistance in times of resilience, in J. Butler, Z. Gambetti and L. Sabsay (eds), *Vulnerability in Resistance* (pp. 52–75). Durham, NC: Duke University Press. https://doi.org/10.1215/9780822373490-004

Brazell, M. (2017). Was Macht Uns Wirklich Sicher? Toolkit Für Aktivist_innen, in *Was Macht Uns Wirklich Sicher? Toolkit Für Aktivist_innen*. Available at: https://ia902900.us.archive.org/18/items/toolkit-was-macht-uns-wirklich-sicher/toolkit-finished-1.pdf. (Accessed 1 September 2023).

Brazell, M. (2021). Von Negativer/Strafrechtsfeministischer Zu Positiver/Abolitionistischer Sicherheit: Transformative Gerechtigkeit Für Betroffene von Geschlechtsbasierter Gewalt, in M Laufenberg and Vanessa E. Thompson (eds), *Sicherheit: Rassismuskritische und Feministische Debatten, Forum Frauen-Und Geschlechterforschung* (pp. 328–363). Münster, Germany: Westfälisches Dampfboot.

Butler, J. (2006). *Precarious Life: The powers of mourning and violence*. New York, NY: Verso.

Butler, J. (2020). *The Force of Nonviolence: An ethico-political bind*. New York, NY: Verso Books.

Butler, J., Gambetti, Z. and Sabsay, L. (eds). (2016). *Vulnerability in Resistance*. Durham, NC: Duke University Press. https://doi.org/10.1215/9780822373490

Clark-Parsons, R. (2018). Building a digital Girl Army: The cultivation of feminist safe spaces online. *New Media & Society,* 20(6), 2125–2144. https://doi.org/10.1177/1461444817731919

Cockburn, C. (1988). *Machinery of Dominance: Women, men, and technical know-how*. Boston, MA: Northeastern University Press. https://doi.org/10.3406/apre.1988.864

Coleman, E. G. (2013). *Coding Freedom: The ethics and aesthetics of hacking*. Princeton, NJ: Princeton University Press. https://doi.org/10.1515/9781400845293

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

Dorlin, E. (2022). *Self-Defense: A philosophy of violence*. New York, NY: Verso.

Dourish, P. and Anderson, K. (2006). Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction,* 21(3), 319–342. https://doi.org/10.1207/s15327051hci2103_2

Eghbal, N. (2016). Roads and bridges: The unseen labor behind our digital infrastructure, *Ford Foundation*. Available at: https://www.fordfoundation.org/wp-content/uploads/2016/07/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure.pdf. (Accessed 1 September 2023).

Eikren, E. and Ingram-Waters, M. (2016). Dismantling 'you get what you deserve': Towards a feminist sociology of revenge porn. *Ada: A Journal of Gender, New Media & Technology*, 10, 1–19.

Fairbairn, J. (2015). Rape threats and revenge porn: Defining sexual violence in the digital age, in V. M. Steeves and J. Bailey (eds), *EGirls, ECitizens* (pp. 229–251). Ottawa, Canada: University of Ottawa Press.

Federici, S. (2019). Social reproduction theory, *Radical Philosophy*, 204, 55–57.

Fernandez, M. and Wilding, F. (2003). Situating cyberfeminisms, in M. Fernandez, F. Wilding and M. M. Wright (eds), *Domain Errors! Cyberfeminist practices* (pp. 17–28). New York, NY: Autonomedia.

Folkers, A. and Langenohl, A. (2020). Editorial: Was ist sorgende Sicherheit? *BEHEMOTH A Journal on Civilisation,* 13(12), 1–15. https://doi.org/10.6094/BEHEMOTH.2020.13.2.1043

Gentry, C. E., Shepherd, L. J. and Sjoberg, L. (eds) (2019). *The Routledge Handbook of Gender and Security*. London (UK); New York (NY): Routledge, Taylor & Francis Group. https://doi.org/10.4324/9781315525099

Hansen, L. and Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, 53(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Haraway, D. (1987). A manifesto for Cyborgs: Science, technology, and socialist feminism in the 1980s. *Australian Feminist Studies*, 2(4), 1–42. https://doi.org/10.1080/08164649.1987.9961538

Harding, S. G. (ed) (2004). *The Feminist Standpoint Theory Reader: Intellectual and political controversies*. New York, NY: Routledge.

Hill Collins, P. (2000). *Black Feminist Thought: Knowledge, consciousness, and the politics of empowerment*. Rev. 10th anniversary ed. New York, NY: Routledge.

Jasanoff, S. (2015). Future imperfect. Science, technology, and the imaginations of modernity, in S. Jasanoff and K. Sang-Hyun (eds), *Dreamscapes of Modernity. Sociotechnical imaginaries and the fabrication of power* (pp. 1–33). Chicago, IL: University of Chicago Press. https://doi.org/10.7208/chicago/9780226276663.003.0001

Kämpf, K. M. (2014). Safe spaces, self-care and empowerment – Netzfeminismus im Sicherheitsdispositiv. *FEMINA POLITICA – Zeitschrift für feministische Politikwissenschaft*, 23(2), 71–83. https://doi.org/10.3224/feminapolitica.v23i2.17615

Kleiner, D. (2010). *The Telekommunist Manifesto*. Network Notebook 3. Amsterdam, Netherlands: Institute of Network Cultures.

Lange, G. M. and wessalowski, n. (2023). Doing with Care: Feministische Datenpraktiken, in C. Brunner, G. Lange and n. wessalowski (eds), *Technopolitiken der Sorge* (pp. 147–170). Vienna, Austria: Transversal Texts.

Laufenberg, M. and Thompson, V. M. (2021). Kritik der Sicherheit Gesellschaftstheoretische und intersektionale Perspektiven, in M. Laufenberg and V. M. Thompson (eds), *Sicherheit: Rassismuskritische und feministische Beiträge*. Münster, Germany: Westfälisches Dampfboot.

Loick, D. (2021). 'Das Grundgefühl der Ordnung, das alle haben.' Für einen queeren Begriff von Sicherheit, in M. Laufenberg and V. M. Thompson (eds), *Sicherheit: Rassismuskritische und feministische Beiträge*. Münster, Germany: Westfälisches Dampfboot.

Lorey, I. (2015). *State of Insecurity: Government of the precarious* (translated by A. Derieg). London (UK); New York (NY): Verso.

Lowenhaupt Tsing, A. (2017). *The Mushroom at the End of the World*. Princeton, NJ: Princeton University Press.

Moore, J. W. (2016). *Anthropocene or Capitalocene? Nature, history, and the crisis of capitalism*. Birmingham, NY: PM Press.

Pavlona, P. (2021). Human rights defenders in cyberspace: A litmus test for cybersecurity, *Global Policy Journal*, 5. Available at: https://www.globalpolicyjournal.com/blog/11/05/2021/human-rights-defenders-cyberspace-litmus-test-cybersecurity. (Accessed 1 September 2023).

Peña, P. and Varon, J. (2019). Consent to our data bodies: Lessons from feminist theories to enforce data protection, *Coding Rights*, March 2019.

Petty, T. (2016). Safety vs security: Are you safe or are you secure?, in T. Lewis, S. P. Gangadharan, M. Saba and T. Petty (eds), *Digital Defense Playbook: Community power tools for reclaiming data* (pp. 82–83). Available at: https://www.odbproject.org/wp-content/uploads/2019/03/ODB_DDP_HighRes_Spreads.pdf. (Accessed 1 September 2023).

Pierce, J., Fox, S., Merrill, N. and Wong, R. (2018). Differential vulnerabilities and a diversity of tactics: What toolkits teach us about cybersecurity, in *Proceedings of the ACM on Human-Computer Interaction 2 (CSCW)* (pp. 1–24). https://doi.org/10.1145/3274408

Powell, A., Flynn, A. and Sugiura, L. (eds) (2021). *The Palgrave Handbook of Gendered Violence and Technology*. Cham, Switzerland: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-83734-1

Radloff, J. (2013). Digital security as feminist practice. *Feminist Africa*, 13, 145–155. Available at: https://genderlinks.org.za/wp-content/uploads/imported/articles/attachments/20137_fa18_web-1.pdf#page=153. (Accessed 1 September 2023).

Raghavan, S. and Hussen, T. S. (eds.) (2023). *Global Attention to Technology-Facilitated Gender-Based Violence (TFGBV): Feminist perspectives*. Available at https://www.genderit.org/editorial/global-attention-technology-facilitated-gender-based-violence-tfgbv-feminist-perspectives. (Accessed 1 September 2023).

Reagle, J. (2014). The obligation to know: From FAQ to Feminism 101. *New Media & Society*, 18(5), 691–707. https://doi.org/10.1177/1461444814545840

Robles, G., Reina, L. A., Gonzáles-Barahona, J. and Dueñas Domínguez, S. (2016). Women in free/libre/open source software: The situation in the 2010s, in *Open Source Systems: Integrating Communities: 12th IFIP WG 2.13 International Conference, OSS 2016, Gothenburg, Sweden, May 30 - June 2, 2016, Proceedings* (pp. 163–173). Cham, Switzerland: Springer International Publishing. https://doi.org/10.1007/978-3-319-39225-7

Rouvroy, A. (2013). The end(s) of critique: Data-behaviourism vs. due-process, in M. Hildebrandt and K. De Vries (eds), *Privacy, Due Process and the Computational Turn: The philosophy of law meets the philosophy of technology* (pp. 143–167). New York, NY: Routledge.

Schatz, D., Bashroush, R. and Wall, J. (2017). Towards a more representative definition of cyber security. *The Journal of Digital Forensics, Security and Law*, 12(2), 53–74. https://doi.org/10.15394/jdfsl.2017.1476

Sedgwick, E. K. (2003). Paranoid reading and reparative reading, or, you're so paranoid, you probably think this essay is about you, in M. Barale, J. Goldbergand and M. Moon (eds), *Touching Feeling: Affect, pedagogy, performativity* (pp. 123–152). New York, NY: Duke University Press. https://doi.org/10.2307/j.ctv11smq37.9

Shnayien, M.-L. (2022). *Die unsicheren Kanäle: Negative und queere Sicherheit in Kryptologie und Informatik*. Bielefeld, Germany: Transcript Verlag. https://doi.org/10.14361/9783839463062

Slupska, J. (2019). Towards a feminist critique of cybersecurity. *St. Anthony's International Review*, 15, 83–100. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3429851. (Accessed 1 September 2023).

Spideralex. (2023). Feministische Infrastruktur Aufbauen: Helplines Zum Umgang Mit Geschlechts-Spezifischer Gewalt Im Internet', in C. Brunner, G. M. Lange and n. wessalowski (eds), *Technopolitiken Der Sorge* (pp. 55–78). Vienna, Austria: Transversal Texts.

Srnicek, N. (2017). *Platform Capitalism*. Theory Redux. Cambridge, UK: Polity.

Strohmayer, A., Bellini, R. and Slupska, J. (2022). Safety as a grand challenge in pervasive computing: Using feminist epistemologies to shift the paradigm from security to safety. *IEEE Pervasive Computing*, 21(3), 61–69. https://doi.org/10.1109/MPRV.2022.3182222

Suárez-Gonzalo, S. (2019). Personal data are political. A feminist view on privacy and big data. *Recerca. Revista de Pensament i Anàlisi*, 2(24), 173–192. https://doi.org/10.6035/Recerca.2019.24.2.9

Toupin, S. and Spideralex. (2018). Introduction: Radical feminist storytelling and speculative fiction: Creating new worlds by re-imagining hacking. *Ada: A Journal of Gender, New Media, and Technology*, 13. https://doi.org/10.5399/uo/ada.2018.13.1

Tronto, J. C. and Fisher, B. (1990). Toward a feminist theory of caring, in E. Abel and M. Nelson (eds), *Circles of Care*. Albany, NY: SUNY Press.

UNESCO. (2019). *I'd blush if I could: Closing gender divides in digital skills through education*. Available at: https://www.empowerwomen.org/en/resources/documents/2019/05/id-blush-if-i-could-closing-gender-divides-in-digital-skills-through-education?lang=en. (Accessed 1 September 2023).

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Veale, M. and Brown, I. (2020). Cybersecurity. *Internet Policy Review*, 9(4). https://doi.org/10.14763/2020.4.1533

Vickery, J. R. (2018). This isn't new: Gender, publics, and the Internet, in J. R. Vickery and T. Everbach (eds), *Mediating Misogyny* (pp. 31–49). Cham, Switzerland: Springer International Publishing. https://doi.org/10.1007/978-3-319-72917-6_2

Wajcman, J. (2004). *TechnoFeminism*. Cambridge, UK: Polity Press.

Zaharijević, A. (2013). How to know a citizen when you see one? The sex of a citizen. *Identities: Journal for Politics, Gender and Culture*, 10(1–2), 71–82. https://doi.org/10.51151/identities.v10i1-2.282

Zakharova, I. and Jarke, J. (2024). Care-ful data studies: Or, what do we see, when we look at datafied societies through the lens of care? *Information, Communication & Society*, 27(4), 651–664. https://doi.org/10.1080/1369118X.2024.2316758

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power*. New York, NY: PublicAffairs.

Citation: wessalowski, n., Lange, G. M. and Kannengießer, S. (2025). A Feminist Critique of Cybersecurity: Technofeminist Imaginaries of Vulnerability and Care. *Feminist Encounters: A Journal of Critical Studies in Culture and Politics*, 9(2), 25. https://doi.org/10.20897/femenc/16783