

THE GENDERED DIMENSIONS OF AI-DRIVEN SECURITY*

Muskan Moazzam and Haris Bilal Malik *

ORCID ID: 0009-0000-4182-7491 and 0000-0001-9410-6575

Declaration*

Abstract

This chapter is a critical analysis of the implications of AI-based security systems on gender and power. It states that so-called neutral technologies in fact carry and enhance the previous prejudices. In all parts of the world, AI is employed in national defense, and domestic surveillance, but it remains a reflection of the values and the blind spots of the developers. Algorithms and policies tend to be quite militarized and state-focused in the security sphere, disregarding the daily requirements of women and the marginalized populations. We integrate feminist international relations theory and new work on AI and cybersecurity to demonstrate that the existing systems do not often pose the question of “whose security is at stake”? or “if the security of the most vulnerable groups is ensured?” Facial-recognition technology, as an example, is much less effective with women and dark-skinned individuals. Females are the disproportionate victims of online harassment and doxxing. Even protective measures, such as CCTV in women’s shelters, frequently become new avenues on which abuse of surveillance is exercised. The Global South particularly is affected by this issue, as the gendered digital inequalities and imported, uniform (“one-size fits all”) cyber policies exacerbate underlying actual disparities in the offline world. Using an intersectional feminist lens, we argue that “security” must be redefined as empowerment rather than control. Co-created policies should embed inclusion, dignity, transparency, and accountability into AI and cyber-governance. Practical principles include gender-aware threat models, diverse decision-making teams, South-South collaboration, and proactive digital inclusion. We conclude that feminist approaches do not weaken security; they strengthen it by making systems more just, humane, and resilient to the needs of those historically at risk.

Keywords: AI security, Gender bias, Feminist International Relations’s Theory, Cybersecurity, Surveillance

* This is the full text of the paper presented at the 9th Cybersecurity Conference.

* Both author Research Associate, Institute of Strategic Studies Islamabad (ISSI), muskanmoazzam7@gmail.com, harismalik000@gmail.com

* This article has been prepared without the use of any Artificial Intelligence (AI) tools or assistance.



Introduction

Artificial intelligence (AI) is being integrated in national security, law enforcement, and the global cyber-governance at an accelerated pace. (OECD, 2019; UNESCO, 2021). This integration also broadens their applications in the military (Scharre, 2018) (Identifying and targeting), in which machine learning is used to determine potential targets. This has also incentivized domestic usage by governments for surveillance by deploying these technologies in public spaces. They are commonly presented as impartial and objective tools, however, in practice, they are known to shape and influence online behaviour, regulate access to power, and contribute to vulnerability (APC, 2020; UNESCO, 2021). Stated differently, AI mirrors social values and hierarchies of the social groups that create it. Gender relations on the internet, such as online gender dynamics have been demonstrated to strengthen or even enhance offline disparities (APC, 2020; Buolamwini & Gebru, 2018). In such a way, a critical gender analysis of AI-powered security could demonstrate some latent power structures and subtle violence that traditional methods fail to detect (Tickner, 1992; Enloe, 2014). The analysis is grounded within feminist international relations lens and human security theory to support the arguments laid out.

The study will be based on a qualitative and interdisciplinary research methodology to perform a critical review of scholarly sources, policy reports, and news sources on AI, cybersecurity, and gender (Creswell & Creswell, 2018). This literature will be analyzed through the prism of feminist international relations and critical security studies, especially the concepts of intersectionality (Crenshaw, 1989); how identity factors such as gendering, racially and in classes influence experience and human-centered security (United Nations Development Programme [UNDP], 1994). By drawing on both theoretical works and tangible evidence, we endeavor to cast the human aspects of AI regulation in the limelight that are usually marginalized within dimensions of AI governance models.

The theoretical framework for this study will be based on feminism school of thought. As per the feminist theorists, the security is neither a goal nor a gender-neutral term. Rather, it is a political and socially constructed term (Tickner, 1992; Enloe, 2014; Ferl & Perras, 2024). The mainstream security paradigm has long been focused on the state, borders, and military force which is a male paradigm that places states as protectors and people (particularly women) as the vulnerable (Tickner, 1992). As a matter of fact, the discussion of digital security has been influenced by a rather homogenous- white and male - group, i.e., the voices of the women and other voices are pushed to the background as an example, decision-makers have been



discovered to set cybersecurity objectives without including women or minorities, meaning that the solutions to the policies are targeted at the ancient power structures instead of real human security. (Brown & Pytlak, 2020; Ferl & Perras, 2024). Feminist IR thus offers a critique of the conventional protector-protected scheme of security, calling out that it must be transferred to more democratic ideas of human security (Enloe, 2014; Tickner, 1992).

We use these concepts throughout this chapter by posing the following questions: 1) What bodies are covered by security? 2) Who are surveilled or attacked, and how identity factors (gender, race, and class, etc.) interfere in digital space? We develop out of such a framework as the Women, Peace and Security agenda of the UN, (United Nations Security Council [UNSC], 2000) as well as feminist foreign policy, (Thompson & Clement, 2019) which remind us that threats may be structural, daily, and gendered, and not necessarily military. The normative objective that we pursue is a feminist digital security paradigm: one that understands security as empowerment, (Hudson, 2005; Tickner, 1992) is made in collaboration with the communities affected, and one that incorporates dignity and inclusion into AI systems at its core.

Literature Review

Feminist Security Studies: Feminist IR literature has maintained that traditional security studies do not pay attention to the experiences of half the population. Theorists (Tickner, 1992; Enloe, 2014; Sjoberg, 2010) who are considered pioneers of the field demonstrated that the concept of traditional security is highly gendered (Tickner, 1992; Enloe, 2014; Ferl & Perras, 2024); it is shaped by masculine militarism and conceals the mechanisms of violence and power at home or on a psychological scale. As an example, feminist theorists suggest that violence is a continuum (Cockburn, 2004); in addition to physical violence, structural, cultural, and everyday violence (e.g., domestic violence, disinformation, etc.) are also a part of the same systemic control of the body and voice of women and marginalized individuals (Ferl & Perras, 2024; Lipede, 2025). When this is applied to the cyberspace, it would be possible to argue that online harms (sexual harassment, doxxing, disinformation, etc.) are part of the same systemic control of the body and voice of women and the marginalized (UN Women, 2023).

Studies also indicate that there is a close connection between the rate of women representation and larger peace/security results (UN Women, 2022). Peace process (UN Women, 2015) studies discover that gender-sensitive policies are likely to be attained when women are



involved in the process. Through analogy, by adding women into cyber and AI policies-making, the latter would be more sensitive to various needs. However, in reality, female representation in cyber diplomacy, cybersecurity occupations, and disarmament talks is simply enormous (Ferl & Perras, 2024; APC, 2020). Indicatively, women have made up of 20-24 percent (UNIDIR, 2023) of the delegates in major UN cyber and AI forums over the last few years (Ferl & Perras 2024). This bias implies that the gender perspectives are not easily listened to. According to one PRIF analysis, the culture of security and technology (PRIF, 2024) has been discussed within paradigms of supposed gender-neutrality which are highly male-centric and militarized. We thus anticipate that the feminist theory will reveal how current AI-security policies promote existing power structures and not general safety.

Gender and Cybersecurity: The current body of literature on gender and cybersecurity demonstrates that the experiences of men and women (APC, 2020) on the Internet may vary significantly, although the technical aspect appears to be unbiased. As an example, gender is at work in the online environment (what is sought and shared), and social networks tend to reproduce the structure of power in the real world. Most recent studies are focused on two topics gender-based online violence (UN Women, 2023) (e.g. hate speech, cyberstalking against women) and gender inequality in the ICT workforce. Both apply to security. It is also evident that a significant percentage of women across the world have encountered any form of digital harassment [uneca.org](https://www.uneca.org), but these do not feature in the conventional cyber policy agendas. In the meantime, the proportion of women as cybersecurity professionals is low, (ISC², 2023) just 24 percent of the professionals worldwide, with smaller percentages among technology-based jobs and managerial positions and leadership. It implies that it is common that cybersecurity policies are made and enforced by male-dominant teams, which are unaware of such issues like online domestic abuse or algorithmic discrimination.

Important reports focus on the fact that cybersecurity is inherently connected (Office of the High Commissioner for Human Rights, 2022) with human rights, as well as that gender is a major factor of vulnerability. An instance is a 2020 report by feminist researchers claiming that there is a gender issue to international cyber security since it is based on the broader structural inequalities and that it needs a comprehensive response. Online gender-based violence (GBV) - including image-based abuse to doxxing - has been found to be instilled by structural inequalities. Nevertheless, global cyberspace discourses tend to divide cyberspace security and human rights, that is, the harmful effects on gender are under-investigated. Concisely, literature provides evidence that the harms of online are gendered, and the



protection of human rights (including women rights) is particularly important in the context of cybersecurity policyapc.org uneca.org.

AI and Gender: There is an increasing amount of literature analyzing the ways AI recreates gender (and racial) stereotypes (UNESCO, 2021). What machine-learning models learn is information that is guided by historical stereotypes (Buolamwini & Gebru, 2018). As an example, computer-vision research has shown that facial-recognition systems (Buolamwini & Gebru, 2018) are highly effective with white men but they miss by a large margin with women of color (Young Women's Movement, nd). This intersectional bias implies that the AI-based police and surveillance systems falsely identify or overlook non-white, female victims disproportionately. (UN Women, 2023; APC, 2020). In the same manner, the language-processing algorithms (UNESCO, 2021) tend to fall back to the usage of male pronouns when addressing things such as doctor or CEO, which perpetuates sexist associations. Gender bias in AI can be disastrous in terms of security. A recent study reports that close to 45 percent of the machine-learning systems reviewed are gender-biased (and more than 25 percent are gender and racial-biased) (Ferl & Perras, 2024). Any bias, no matter how minor, is perilous in military AI: an autonomous targeting system, which is skewed to recognize only military-aged men, can miss female combatants or civilian women in war-torn areas. Besides, emerging AI-powered threats such as deepfake pornography (UN Women, 2023) pose new gendered threats: fake images and videos can be used as an instrument of the so-called image-based sexual violence, which will predominantly harm women and their reputations and safety.

This is how a feminist view cautions that unless it is diverse, AI will merely replicate and amplify the existing inequality (Ferl & Perras, 2024). Moral AI ethics initiatives remind that to avoid gender bias in AI; we first need to address gender bias in our society. Practically, it involves the need to have varied development teams (OECD, 2019) and training information incorporating women, minorities, and Global Souths views. The literature, therefore calls on gender-conscious AI design and governance: developing algorithms and policies that are conscious of various social groups and do not reinstate old hierarchies.

Online Harassment and Surveillance: Related literature shows that digital threats affect women (UN Women, 2023) in a unique way. UN Women states that 16-58 percent of women all over the world have been victims of digital violence- the number spans both online harassment and stalking as well as non-consensual sharing of intimate images (Lipede, 2025).



Crucially, this is not the online violence, but it has severe consequences in real life (trauma, loss of career, threats to physical safety). The critical discussions by the scholars note that digital violence (Association for Progressive Communications, 2020) is inherently gendered: activists, journalists, and young women are more likely to be the victims of it, which can be explained by the occurrence of the patriarchal norms. As an example, an APC report states that online doxxing of women can lead to the threat of death or rape in real life (APC, 2020).

Ironically, most of the so-called protective technologies increase the state and individual surveillance on women. Feminist critics have been able to highlight such instances as the use of hidden cameras in women shelters or salons- supposedly to ensure safety but only to blackmail or harass the residents (Ali, 2024). Accordingly, the literature postulates that in the absence of a gender lens, the digital security provisions may work against them, making women spaces a location of control instead of safety.

In general, the historical studies are united around the point that technology, security and gender are self-affirming concepts. Feminist reading further demands that cybersecurity should extend (Hudson, 2005) past the militaristic defense and human security, taking into account such concerns as privacy, community coherence, and the absence of harassment. That insight is further developed in this chapter to examine AI-driven security in particular.

7

Analysis and Discussion

Human Security vs. State-Centric security

The main issue with this is that the majority of cyber and AI security frameworks are still state-centric (UNDP, 1994) and militarized concepts of security. Instead of concentrating on individual or community wellbeing, they concentrate in border control, deterrence, (Tickner, 1992) and national infrastructure- which are the traditional areas of military strategy. Since one commentator notes, international security remains heavily defined by state- and military-based security and structural violence, gendered aspects of which have been left out (Ferras & Perras, 2024). Security in this kind of paradigm means surveillance, to find the presence of foreign threat or repression of dissent at the cost of citizen rights. The key focus of cyber strategies is secrecy, offense/defense capability, and global competitiveness, which do not give much space to issues such as online gender-based violence or data privacy of vulnerable groups.



That leads to the question; whose security is it? (Enloe, 2014). Feminist response: almost always the safety of the already powerful (of states, armies, elites) and not of ordinary people. Vernacular structures seldom pose the question of whether the women, LGBTQ+, ethnic minorities or the poor are safer in these structures. As an illustration, predictive policing (Richardson, Schultz, & Crawford, 2019) tools are meant to forecast the crime location, although they tend to utilize data filled with bias, that shows historical over-policing of marginalized group. Equally, border-control algorithms can be used to monitor immigrants or refugees (UNHCR, 2022) and disregard digital risks to displaced women like fake online up to the scam or harassment of refugees. The consequence is that the gains of the security (such as order in the country or national stability) are distributed unevenly whereas the costs (data mining invasion, false allegations) are incurred by the weakest.

AI as a Mirror of Society

Artificial intelligence is often portrayed as a neutral (UNESCO, 2021) decision-maker, but in fact it acts as a mirror of the society that built it. Any algorithm trained on historical data (Barocas & Selbst, 2016) will absorb patterns of inequality in that data. In the security realm this is especially treacherous. For instance, widely used facial recognition (Buolamwini & Gebru, 2018) systems have been demonstrated to identify white male faces with very high accuracy, yet they often *fail to recognize Black women's faces*. This is not a technical quirk but a systemic bias: the training sets and design priorities were skewed toward one demographic. When law enforcement deploys these cameras, women and people of color may find themselves wrongly flagged or ignored, undermining both fairness and safety. (Young Women's Movement, 2025)

The bias is not limited to vision. Natural language processing can encode stereotypes (Bolukbasi et al., 2016) (e.g. associating careers with men), and allocation algorithms (for credit, jobs, or policing resources) can disfavor marginalized groups. Crucially, security is about threats – but what counts as a threat is itself gendered. A male-centric policy might see only traditional men-in-uniform as combatants, ignoring how women could both be combatants or victims. As one study points out, if autonomous targeting systems carry gender biases, “*‘military-aged men’ will most likely be disproportionately miscategorized as combatants and thus as potential targets*”. Meanwhile, crimes that mainly affect women (like domestic violence or online harassment) might not even register as “cybersecurity” issues, so they go unmodeled by threat-detection algorithms.



Crucially, technology also creates new gendered threats. The advent of deepfake technology (UN Women, 2023) – AI-generated images and videos – has led to a surge in “image-based sexual violence.” Women are disproportionately victims of deepfake pornography, which is harder to police and can ruin reputations and careers. In addition to this, artificial intelligence is deployable to produce tailored disinformation. Misogynistic propaganda or anti-LGBTQ propaganda is propagated by automated bots (UNESCO, 2023) and tends to silence women in the general conversation. These emergent harms elucidate that cybersecurity cannot continue to exist in the technical sense; it must also confront gendered social forces.

Gendered Impacts of AI-Driven Security

The practical consequences of ignoring gender in AI security are manifold. We highlight a few illustrative domains:

Predictive Policing and Surveillance: AI-driven surveillance tools (from predictive policing (Richardson et al., 2019) algorithms to license-plate readers) tend to target poor and minority neighborhoods, which also often have higher numbers of women and children in precarious situations. Attack and targeting in socio-political context might subject whole communities to greater scrutiny. Predictive policing systems, including PredPol, have been studied empirically to show that a feedback loop of biased input, e.g. a history of over policing, can create a vicious cycle, where the algorithm will seemingly anticipate more law-enforcement presence in already heavily-surveilled districts (Young Women’s Movement, 2025). Such a vested relationship is more than problematic in environments marked by cannibalistic gendered inequities where so many women are already facing domestic violence or have inadequate access to vital support.

Facial Recognition Bias: Computer vision studies consistently find that facial-recognition software has higher error rates for women and especially for women of color (Buolamwini & Gebru, 2018). This has two implications: women may be wrongly flagged by security systems (leading to humiliating stops or arrests) or worse, not identified when needed (e.g. if a missing child has a photo on file). If those systems are trained on biased data, they could exacerbate gender and racial profiling within the country’s growing surveillance apparatus.

Online Harassment and Cyberstalking: Women in all societies face higher rates of certain digital harms. UN Women reports that 16–58% of women (UN Women, 2023) and girls have experienced some form of digital violence (online harassment, stalking, non-consensual



image sharing) (Lipede, 2025). This violence is strongly linked to offline gender norms: a woman speaking out publicly online may invite sexist threats that aim to silence her. These threats are security issues too – they create fear and inhibit half the population from participating fully in the digital sphere. Moreover, online abuse often spills into offline life. For example, the APC report notes that being doxxed (having personal data published) has escalated into women receiving in-person rape and death threats (APC, 2020). Yet conventional cybersecurity frameworks often treat these as “private” or legal issues rather than security matters. The slide rightly notes that issues like doxxing, harassment, and cyberstalking, which overwhelmingly affect women, remain under-prioritized in cyber policy agendas, making cyberspace a hostile environment for women.

Protective Measures Becoming Surveillance: Paradoxically, some measures introduced to “protect” women have backfired by subjecting them to new surveillance. The Dawn report on Pakistan describes CCTV cameras being installed in women’s shelters, hostels, and even beauty salons – ostensibly for security – but then misused by staff or intruders to record and blackmail residents. In these cases, technology meant to provide safety actually invaded private spaces, creating “a hostile environment of mistrust and insecurity” among women (Ali, 2024 & Privacy International, 2021). These instances illustrate a pattern: without careful oversight, AI-driven tools tend to expand policing into everyday life, frequently without consent or accountability.

Taken together, these impacts show that an AI-driven security regime can worsen the situation for many women and marginalized people, even as it purports to protect the population as a whole. Biased algorithms reinforce existing structural inequalities, turning the digital sphere into an extension of offline power imbalances.

The Global South Perspective

These issues are compounded by other factors in the Global South. One is that technical policies and systems are often brought in from the North without adequate localization. Numerous countries have adopted cyber security frameworks (UNESCO, 2021) and AI tools from other countries, believing they will be effective in their own country. However, threats and social contexts are different. South Asia and Africa are where gendered disinformation campaigns on the Internet and mobile economies of harassment are considered serious issues, but not ones engaged by imported policies. Making digital security local-to-life is difficult for



women's movements in these areas. Another observer's words capture the offline inequities in the Global South that "replicate themselves online" (APC, 2020).

Second, there are significant gender disparities in Internet use and digital literacy in most countries in the Global South. Only around 48% of women in the world use the internet (as opposed to 58% of men) and the gap is much higher in some areas such as South Asia and Africa (ITU, 2023; GSMA, 2024).

Third, there is an underrepresentation (UNIDIR, 2023) of women in regional processes of AI and cyber policy. Few (if any) women are part of advisory boards on technology or cybersecurity in many governments in the Global South. This disparity ignores matters such as gendered harassment, data privacy for survivors of violence, gender-responsive algorithms, and more.

Finally, there are specific risks for the Global South that don't always get noticed. One such example that has been found is the use of AI to spread misinformation about women's rights or reproductive health matters, which is more prevalent in certain regions, such as India and Pakistan, and is not a topic that typically comes to mind with cybersecurity concerns. In certain countries, such as Brazil and India, deepfakes have been employed in harassment campaigns. These risks are not mitigated because they do not have inclusive data or threat models. This leads to a "digital power divide" (World Bank, 2023) in which the offline status quo of women as subjects of subjugation in education, economy and law becomes the same status quo in cyberspace (Ali, 2024). To sum up, current inequalities of a patriarchal and postcolonial nature are being inscribed into cyber space if we do not do something about it.

Given that today's cyber policies fail to pass the gender test, what can be done?

These gendered aspects are not being addressed by the existing national and international cyber strategies. The majority of frameworks focus on deterrence, secrecy and state sovereignty – which excludes individual wellbeing. It is common to hear little or no mention of human security, if it is mentioned at all. For example, while the discussion of cybersecurity has been about critical infrastructure protection, data confidentiality for businesses or strategic cyber defense, it does not necessarily pay much attention to the harms when they occur at the community level. In cybersecurity, as with so many other areas, a "largely male-centric... view" that "often overlooks the unique experiences, expertise, and vulnerabilities of women and other marginalized groups" (Ferl & Perras, 2024) reigns supreme.



A case in point is international cyber diplomacy. As UN groups or summits on emerging tech gather, there is little representation from women, gender advocates say. The problems they talk about are never social justice issues, but technical puzzles or national security puzzles. At present, policies to date have little on the agenda to protect gendered data (such as reproductive health data), to regulate harassment enabled by AI, and to support the victims of online harassment. The mention of gender occurs mostly when looking at more ways to include women (a narrow “add women” approach) and not when considering (re)thinking threat models.

The slide “security becomes synonymous with surveillance, while safety remains neglected” is well-suited. In fact, in many states, investing in AI surveillance or digital protection will automatically ensure the protection of all citizens, but evidence indicates that only the powerful will be protected. Different measures are needed to gauge women's real security – their freedom from violence, abuse, and exclusion. The current policies leave out the emotional and social issues such as everyday concerns for girls and women to be followed on social media and their private lives to be exposed due to data breaches. To put it simply, the mainstream focus on security is technical, not social, and it's neglecting half the people.

Toward a Feminist Digital Security Paradigm

So what would a feminist security framework be if it failed in these ways? First and foremost, it restates the concept of security as empowerment, rather than control (Hudson, 2005). Rather than “How can we watch people better?”, it asks “How can we keep people safe in ways that respect their dignity?” The focus on security policy would no longer just be on crisis management but on developing resilience – such as through digital literacy, community networks, and support for online vulnerable groups.

Creating policies and technologies together with the communities they are meant for, rather than being imposed from above is inclusive co-creation (OECD, 2019). This includes the engagement of women, gender minorities and other marginalized groups in every stage: from threat assessment to system design and governance. An example of a smart city surveillance system would be the creation of a system only after taking the concerns of women's rights into account as well as the placement of surveillance cameras away from sensitive areas. The APC report warns that the inclusion of women in negotiation processes increases the likelihood of gender provisions being included; and involving a variety of actors in cyber policy increases the chances of identifying blind spots (such as a feminist approach to misinformation).



Transparency and Accountability: AI and security systems need to be transparent and auditable (NIST, 2023). A specific issue is secret algorithms: when a predictive policing tool identifies a neighborhood as being “high risk” the residents should be able to find out why and appeal. Rules and policies must be made explainable (European Commission, 2024) and have ways to counteract biases when using AI to make decisions. This gives the public the power to challenge government and other entities if they are not delivering fair and equitable results.

Gender-aware threat modeling: Threats to security architectures should be gendered (UN Women, 2023). The classic view is threats to infrastructure such as cyberattacks or national espionage. A feminist approach would include online GBV, digital privacy violations (particularly of victims of violence), gendered disinformation and privacy for reproductive data. The PRIF analysis recommends that data breaches of health records should be considered a separate issue, as these breaches can specifically pose risks to women's reproductive rights. Likewise, the potential for the use of AI surveillance apparatus to trap LGBT+ people and minority women should be assessed (e.g. profiles on malicious dating apps used to blackmail vulnerable people). When policies are expanded to include anything that can be construed as a cyber-threat, the policies become more human-centered (Feral & Perras, 2024).

Embedding Diversity: A practical principle is to ensure diversity (UNESCO, 2021) in technical and policy teams. Research on tech organizations shows that homogenous teams are more likely to overlook biases (Feral & Perras, 2024). Therefore, ministries and companies working on AI security should recruit and retain women, people of colour, and Global South experts. We saw in Turkey's context that only 22% of AI professionals are women (Ahmed, 2024); raising this number would help bring feminist insights into the design of new systems.

Global South Collaboration: Feminist tech governance should foster South–South exchanges (UNCTAD, 2023). Countries facing similar challenges (like gendered misinformation in South Asia) can share best practices and co-develop standards. This counters the top-down nature of policy transfers. For example, Pakistan and Turkey might jointly research how to regulate AI-driven deepfakes that target women, and propose regional guidelines that reflect local social norms.

Proactive Digital Inclusion: Lastly, the ultimate need must be to incorporate inclusivity at an early stage. Instead of responding to crises, policymakers and civil society organizations



should invest in empowering women with digital skills and safety connectivity and legal guarantees. Programs that teach digital literacy (ITU, 2023), such as privacy protocols, anti-harassment reporting systems, and critical thinking about fake news, can make people resistant to AI-related dangers. The promotion of women participation in the fields of STEM and security and the creation of grassroots security options, as emphasized by the PRIF blog, is invaluable (Ferl & Perras, 2024). In practice, it may mean funding community technology locations that serve women, finish feminist hackerspaces, or integrate gender-aware cybersecurity education in the K-12 curriculum.

With the support of the general principles, namely, co-creation, transparency, diversity, intersectionality and inclusion, the new paradigm of feminist digital security can be imagined. Justice and empowerment are the key security outcomes that are raised in this paradigm. An example is instead of extending CCTV cameras to try to prevent crime, a feminist approach would focus on sound privacy laws that protect the data of women and invest more in social projects that focus on the causal factors associated with violence. Its end goal is to build a technology ecosystem that empowers the voices of the marginalised groups instead of silencing them.

Principles for Equal Digital Governance

To summarize, key operational principles for an equal (feminist) digital governance model include:

Diverse Representation: Women and minorities deserve to be incorporated in AI policy boards, cybersecurity agencies, and data science teams as this is absolutely necessary (OECD, 2019). Diversity is important to conceive not as a tokenistic inclusion but as a conscious architectural response; the available data represents that diverse teams with a mix of genders developed a more equitable outcome (Ferl and Perras, 2024). The greater representativeness will naturally integrate gender issues into the processes of planning.

Gender-Aware Threat Models: Expenses elaborate threat evaluations that are express in integrating gendered harms (NIST, 2023). As an example, cybercrime units should track the online GBV patterns and work in liaison with the gender-based violence support organizations. The standards of AI should include assessments of bias, including the evaluation of facial-recognition effectiveness in relation to gender and race, before it is used.



Collaboration and Knowledge Sharing: It is necessary to promote the creation of interdisciplinary networks that allow feminist technologists and policymakers to collaborate (UNESCO, 2021) and exchange knowledge both in the Global South and the Global North. The actors of civil society have taken the lead in places (Pakistan, Turkey, and elsewhere) in overcoming digital violence already; official spaces can be very helpful in sharing the best practices, organizing campaigns, and collectively creating gender-sensitive regulatory policies.

From Reactive to Proactive: Switch between crisis response and preventive resilience (European Commission, 2024). Instead of catching the harassers after they occur, we must invest in community education, secure social media design, and empowerment of the at-risk groups. Active approach also involves regular auditing of AI systems to identify emerging vulnerabilities and revision of policies before the damage spreads.

Conclusion

AI-assisted security is an instrument with no neutrality (UNESCO, 2021); conversely, AI becomes very much intertwined with the political sphere and supports pre-existing hierarchies between genders and races. The chapter has followed the way in which the current AI security paradigm, which centers around the power of the state, has continued to obstruct women and other communities historically repressed. Digital security practices reinforce, not reduce, structural inequalities since they are based on biased algorithms (Barocas & Selbst, 2016), a one-size-fits-all policy framework, and a narrow definition of a threat. With the leaders starting to admit (though not necessarily in reality) that artificial intelligence systems can, in fact, enhance the already existing biases, and particularly those that discriminate against women (Ahmed, 2024, & Buolamwini & Gebru, 2018), the importance of a remedy model becomes apparent. However, a feminist approach (Tickner, 1992; Hudson, 2005) provides a path of transformation. A gender-focused and justice-based policy can enhance the resilience system by improving the effectiveness of the system in serving all the stakeholders, instead of compromising security. Once the current thinking of security as empowerment (UNDP, 1994), then technology can be used to fight the causes of violence and insecurity. To act as an example, inclusive AI would be better able to protect the survivors of violence with automated harassment filtering, break privacy traps through diversity in policy-makers, and rally digitally enabled vulnerable communities to develop common defenses. The real security should start with the most vulnerable people at the end. Existing AI systems safeguard the



agendas of major nation-states, senior leadership, corporate entities, and other powerful lobbying organizations, thereby putting other groups at the risk of new types of violence and surveillance. Feminist digital security paradigm, in its turn, does not consider justice, accountability, and inclusion as peripheral matters but makes it its mission. In turn, only by defying the tendency to marginalize any group, AI and cybersecurity may operate in the best way. The construction of the future of AI-premedicated security will thus require the incorporation of human safety and dignity into our algorithms and policies -not through efficiency or power. By doing such, the feminist approaches offer a more humane, fair and efficient security environment to all.

References

- Association for Progressive Communications. (2020). *Technology-facilitated gender-based violence: Making rights and realities visible*. Association for Progressive Communications.
- Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104(3), 671–732.
- Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim code*. Polity Press.
- Bolukbasi, T., Chang, K.-W., Zou, J. Y., Saligrama, V., & Kalai, A. T. (2016). Man is to computer programmer as woman is to homemaker? Debiasing word embeddings. In D. D. Lee, M. Sugiyama, U. Luxburg, I. Guyon, & R. Garnett (Eds.), *Advances in Neural Information Processing Systems* (Vol. 29). Curran Associates.
- Brown, D., & Pytlak, A. (2020). *Why gender matters in international cyber security*. Women's International League for Peace and Freedom & Association for Progressive Communications.
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Proceedings of Machine Learning Research* (Vol. 81, pp. 77–91).
- Cockburn, C. (2004). The continuum of violence: A gender perspective on war and peace. *Women's Studies International Forum*, 27(1), 24–29.



Crenshaw, K. (1989). Demarginalizing the intersection of race and sex: A Black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *University of Chicago Legal Forum*, 1989(1), 139–167.

Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage.

Enloe, C. (2014). *Bananas, beaches and bases: Making feminist sense of international politics* (2nd ed.). University of California Press.

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

European Commission. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Publications Office of the European Union.

Ferl, A.-K., & Perras, C. (2024). *Beyond the code: Unveiling gender dynamics in AI and cybersecurity for international security* (PRIF Spotlight No. 2/2024). Peace Research Institute Frankfurt.

GSMA. (2024). *The mobile gender gap report 2024*. GSMA.

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.

International Telecommunication Union. (2023). *Facts and figures 2023*. International Telecommunication Union.

ISC². (2023). *2023 cybersecurity workforce study*. ISC².

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York University Press.



Office of the United Nations High Commissioner for Human Rights. (2022). *The right to privacy in the digital age*. United Nations.

Organisation for Economic Co-operation and Development. (2019). *OECD principles on artificial intelligence*. OECD Publishing.

Privacy International. (2021). *Safe cities or surveillance cities? The impact of surveillance technologies on women and marginalized communities*. Privacy International.

Richardson, R., Schultz, J., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *New York University Law Review Online*, 94, 192–233.

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton.

Sjoberg, L. (Ed.). (2010). *Gender and international security: Feminist perspectives*. Routledge.

Thompson, L., & Clement, R. (2019). *Defining feminist foreign policy*. International Center for Research on Women.

United Nations Conference on Trade and Development. (2023). *Digital economy report 2023*. United Nations.

United Nations Development Programme. (1994). *Human development report 1994: New dimensions of human security*. Oxford University Press.

United Nations Educational, Scientific and Cultural Organization. (2021). *Recommendation on the ethics of artificial intelligence*. UNESCO.

United Nations Educational, Scientific and Cultural Organization. (2024). *Challenging systematic prejudices: An investigation into bias against women and girls in large language models*. UNESCO.

United Nations High Commissioner for Refugees. (2022). *Global trends: Forced displacement in 2022*. UNHCR.

United Nations Institute for Disarmament Research. (2023). *Gender perspectives in international cyber policy*. UNIDIR.



United Nations Security Council. (2000). *Resolution 1325 (2000): Women, peace and security*. United Nations.

UN Women. (2023). *Technology-facilitated violence against women: Global perspectives and policy responses*. UN Women.

World Bank. (2023). *World development report 2023: Migrants, refugees, and societies*. World Bank.

