PEACE PRINTS
South Asian Journal of Peacebuilding

Cyber Peacekeeping and Gender:
Promise and Perils of Non-Traditional Security

Natallia Khaniejo

Abstract

UN Peacekeeping operations have evolved significantly over the years to become more multidimensional in nature. Simultaneously, with the declaration of cyberspace as a fifth domain of warfare, cybersecurity is now seen as an integral aspect of national security rather than an auxiliary one. Undergirding both these shifts in the security domain is the question of gender vulnerability that remains a complex issue for traditional security and an emerging one for cyberspace. Through the use of deep-fakes, AI generated content, surveillance and targeting mechanisms, this vulnerability is compounded, particularly in the context of conflict regions. This paper examines cyber peacekeeping as a modality to think about these concerns by drawing on current conflicts as a frame of reference. The paper draws on cyber peacekeeping literature to explore the risks and opportunities associated with cyber peacekeeping and best practices that might be considered to prevent reproducing harm in the cyber domain.

Author Profile

Natallia Khaniejo is a Research Analyst with the Cyber Power and Future Conflict Programme at the International Institute for Strategic Studies (IISS). Dr. Khaniejo's research focuses on the impact of Emerging and Disruptive Technologies on society, global governance in cyberspace, disinformation, and the politics of South Asia. She completed her PhD in International Relations from the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.

Cyber Peacekeeping and Gender: Promise and Perils of Non-Traditional Security

Natallia Khaniejo

Introduction

Peacekeeping is one of the most significant tools in the United Nations' arsenal, despite considerable resistance displayed by states to intervention, given sovereignty concerns. At present there are a total of 12 peacekeeping operations with 24 active missions across the world (UN Peacekeeping 2024). While traditional peacekeeping focused on limiting and de-escalating inter-state conflicts, maintaining ceasefires and working towards peace agreements, the mandate has since evolved to deal with a rapidly transforming geostrategic environment. The 1990s first saw a switch to multidimensional/parallel peacekeeping operations that began to take into account intra-state conflict, the protection of civilians in failed states, and targeted or accidental damage from asymmetric security threats (Day 2020).

This widening scope of peacekeeping has been accompanied by a shift in the notion of ontological security for the nation-state which has now also been broadened to include non-traditional security challenges. Nation-states too are reframing their national security priorities and goals in the wake of the emergence of non-traditional security threats like climate security, food security and the protection of critical information infrastructure (CII) that is the physical and virtual systems sustaining governance networks. The rapid democratization and proliferation of Emerging and Disruptive Technologies (EDTs) like Artificial Intelligence (AI) and quantum computing have made tracking and differentiating between traditional and non-traditional threats even more difficult. The dual use nature of these technologies also has led to a shift from notions of digital solidarity to a resurging rhetoric around digital sovereignty which raises severe concerns in the context of countries using technology to silence dissent.

The question of gender, however, remains under emphasized within this widened security discourse within policy spaces. This under-engagement with gender exists at two levels. Firstly, at the functional level, there is still a lack of sustained understanding about the vulnerability of women and marginalized gender identities in the digital spaces, especially during conflict. Secondly, at a more ontological level, discourse on peacekeeping is yet to fully grapple with the masculinist and patriarchal ideas and practices that undergird conflict and peace and how these leeches into cyberspace as well (Consortium on Gender, Security, and Human Rights 2010). This paper finds itself at this tripartite intersection. Therefore, where it attempts to examine the changing nature of peacekeeping, including the potential and the risks involved in the discourse on cyber peacekeeping, it will analyze the importance of integrating gender discourse within both domains digital spaces and (cyber) peacekeeping - to ensure the security of vulnerable populations particularly in conflict.

While the three domains of gender, cyberspace advancements and peacekeeping efforts seem disparate at first glance, this paper hopes to demonstrate not just the importance of viewing the intersections between them in tandem but also the inescapability of doing so moving forward. In order to do so, it begins by looking at the changing nature of the security landscape with an increased integration of cyber and military effects and the vulnerability of the information space in present day conflicts. The paper will then look at the intersection of peacekeeping and cyberspace – the dangers of viewing advancements in cyberspace as a means to an end rather than a domain of its own, and the stalled nature of cyber peacekeeping in the context of both its potential and its risks. Underlying both discussions is the implication of gender not just in the context of cyber peacekeeping but also structurally as part of a larger set of articulations and contestations regarding the pervasive masculinization in security discourse as a whole. The paper concludes, therefore, by looking at the implications for gender vulnerability and empowerment within this discourse and the opportunities and concerns that these changing dynamics hold for peacekeeping operations moving forward.

The paper approaches the topic from a policy-security perspective and therefore views the three discourses of—shifting security narratives in cyberspace, peacekeeping as practice, and gender discourse undergirding the two—within the context of this framework. These issues have been dealt with in a sustained and holistic manner within literature on digital peacebuilding that examines how ‘technologies for peacebuilding and peacebuilding with technology are coproduced’ (Hirblinger et al. 2023). While the paper draws on some of this literature at its core—particularly around arguments of viewing cyberspace and digital technologies as a domain and not simply as a means to an end—it is unable to contend with more interesting foundational and ontological questions raised by this literature that look at the violence of digital technologies themselves and the dangers around the ‘subjunctive nature’ of their expected implementation (Hirblinger 2023).

Cyberspace as the Fifth Domain

In order to understand the shifting nature of cyberspace and its implications for peacekeeping, it is crucial to understand how cyberspace as a domain has become inexorably integrated with national security. Since the early 2010s, countries have identified cyberspace as the fifth domain of warfare (Murphy 2010) and in the western world, cybersecurity has increasingly become a priority for most nation-states.[1] The cornerstone for this shift could be *Stuxnet*[2] which arguably saw the first cyberweapon deployed against a nation's critical infrastructure. Since then, cyberspace has been an active domain of contestation for nation-states and in the aftermath of the Russia-Ukraine war, countries have also been more open about pursuing capabilities not simply around the defensive pole of cyber engagement but the offensive one as well. This is evidenced in the US declarations of 'hunt forward' and 'persistent engagement' doctrines (Fischerkeller and Harknett 2019).

This raises significant ethical questions and concerns regarding the collateral effects of increased cyber-military engagement. There is a lack of consensus regarding threshold setting in the context of a cyberattack and means to ensure attribution and punishment for malicious actors in cyberspace. Furthermore, unlike most traditional weapons, significant advancements in cyberspace have been industry led with private actors playing a driving force in key areas like cybersecurity and cloud computing. This has led to the provision of services by companies like *Microsoft*, *Amazon*, and *Starlink* in the context of the Russo-Ukrainian conflict, which has raised further ethical questions regarding the blurring of the line between combatants and civilians in conflict. Aside from these questions, there are also significant intersectional concerns surrounding cyberspace, security, and ethics.

Firstly, there is a question of asymmetry and misuse if 'cybermilitary' advancements are seen as distinct from 'whole of society' approaches to cyberspace. Hacktivism is a particularly contentious topic in this context as there have been cases where hacktivists have been able to provide safe spaces for dissidents to document and expose human rights violations while also fighting for free and fair elections. During the Arab Spring uprising for example, hacktivists played a key role (particularly in countries like Libya and Tunisia where government internet shutdowns were the norm) to avoid censorship and organize protests (Bellaby 2023). However, there has now been a shift towards state-backed or -sanctioned hacktivism which has turned these tools against the very populations that they were defending initially.

A second significant concern is the issue surrounding the digital divide between the global north and south. This is particularly contentious in the context of norm formation, and the growing role of the private sector in cyberspace. The intervention of private companies in the context of Ukraine

[1] US Department of Defense incorporated it as a new domain in 2011 while NATO followed suit in 2016. As of 2024, most countries have multiple iterations of their cyber-security strategies and for some countries like Germany the term cyber has also been co-opted into their National Security Strategy thereby linking it ideologically with its core base.

[2] Stuxnet is a malicious computer worm that some call the world's first weaponized software or the first cyberweapon. It became infamous in its use to attack Iranian nuclear facilities in 2010, because of the approximately 100,000 computers infected by Stuxnet by the end of 2010, more than 60 percent were located in Iran. According to E Britannica Stuxnet**,** was specifically written to take over certain programmable industrial control systems and cause the equipment run by those systems to malfunction.

has raised significant concerns for countries in the Global South regarding reliance on corporate morality in times of crisis. While Ukraine was an easy choice for companies that associate themselves with the western liberal order, the Israel-Gaza conflict, and if it were to come to that, a Taiwan Straits crisis, would not be as clear cut for companies to navigate. This has led to a resurgence of narratives to move towards cyber sovereignty instead of cyber solidarity at a global level – particularly from countries that feel neglected and left out of the norm formation process (Qiao-Franco 2024). A move towards cyber sovereignty could be significantly detrimental given the risks associated with authoritarian governments using internet shutdowns to completely quell dissent by any means necessary.

Thirdly, there is the question of gendered violence and a rise in the vulnerability of marginal populations in the context of a cyberconflict. Both the military and cyberspace as domains have been traditionally masculinist enterprises with tendencies towards verbal or physical violence against women (Brown and Pytlak 2020). However, this status quo is being challenged using UN Security Council resolution 1325 and its satellite resolutions, reaffirming the importance of women in peace and security, including peacekeeping (UN Women 2000). This has resulted in countries seeking to improve gender balance within their militaries. Also, there has been a shift in female participation in cyberspace and the emergence of feminist and queer solidarities post *the-me-too* movement (Dadas 2020). This brings us to a unique inflection point wherein gender and intersectionality are no longer incidental aspects of national and international security efforts and are becoming embedded and embodied ones.

Non-Traditional Security: A Shifting Landscape

The last few decades have witnessed a sea change in the kinds of threats that are being faced by nation-states with an increased focus on non-traditional security concerns (Caballero-Anthony and Cook 2013) such as climate change and critical information infrastructure protection. As states seek to digitize various aspects of governance from managing citizen data to military modernization these questions of cyber sovereignty versus cyber solidarity will become more complex. Given the criticality of the information space in times of crisis, states are going to use securitization rhetoric to push for stringent measures in the name of sovereignty. Changes to critical information infrastructure and developments in AI are key aspects of these changes with states seeking to enhance resilience across communication lines and develop sovereign AI capabilities.

Resilience here refers to the ability of a country's information infrastructure to withstand both cyber-attacks as well as other physical disruptions like submarine cable cuts. While cyber-attacks may not be singularly devastating modalities of war the way Weapons of Mass Destruction (WMD) are, they nonetheless are effective in crippling physical infrastructure and can be used in tandem with military and kinetic operations to severe effect (Mackinnon and Iyengar 2022). The democratization and proliferation of these tools also raises concerns regarding their usage by malicious individuals and state backed/non-state actors. States increasingly are grappling with a host of critical infrastructure challenges such as – the use of drones for invasive intelligence, surveillance, and reconnaissance (ISR) (Erkanli 2023); the threats from autonomous vehicles to critical infrastructure and gas pipelines (Giannaros et al. 2023); grey zone threats to submarine cables and critical infrastructure advanced persistent threats (APTs) to breach secure networks and access sensitive information; mass exfiltration of citizen data (Ullah et al. 2018); and the use of AI to target social cleavages and reduce trust in government (Brandt 2023).

Disruptive Technologies in Crisis

Currently, both the Russia-Ukraine war and the Israel-Gaza conflict have demonstrated the use of emerging and disruptive technologies in crisis (Sharma 2024). Russia has targeted Ukraine's Critical Infrastructure (Harding, Sabbagh, Koshiw (2022) in much the same way as it did with Crimea in 2014, while also undermining the solidarity of Ukraine's allies through systematic disinformation operations (Digital Forensic Research Lab 2024). Furthermore, geostrategic competition and the rise of US-China tensions has also had an impact on supply chains with states seeking to identify sustainable and diverse supply routes for self-sustainability. Nowhere, has the difficulty of navigating a contested information space been clearer than in the case of Israel-Gaza where navigating even basic information has proved incredibly challenging.

The Israeli Defense Forces (IDF) has engaged in active information operations in an attempt to control and manipulate the narrative of the conflict, including the spread of propaganda regarding the beheading of children, which was irresponsibly repeated by Joe Biden despite remaining unverified (Maad, Forey, Audureau 2024), and the narrative of the storming of Al Shifa hospital. While some of the fake news has been debunked over time, in some cases despite retractions, original pieces are still circulating in cyberspace.

Peacekeeping operations too will need to adapt to the changing nature of these threats that apply in state-state conflict, within conflict regions, and in forcibly displaced/migrant communities as well. Cyber means, whether physical or virtual, are dual edged in their applications. Social media can help proliferate large swathes of information in the case of a public health or environmental crisis but AI, trolls and bots can be used to reduce credibility, target minorities, spread disinformation, and create echo chambers for hate speech and extremist rhetoric to flourish, as was seen in the case of Meta's (then Facebook) inability to monitor and control hate speech against the ethnic Rohingyas in Myanmar (Guzman 2022).

Significant advancements in the field of cyber warfare have also meant an increased vulnerability of civilian populations to cyber-attacks. Historically, unlike conventional forms of warfare, cyber-attacks were often seen as less threatening in terms of their physical effects. In the current landscape however, this is no longer the case, and such collateral damage could cause a significant amount of financial loss aside from individual or personal losses. For instance, a hypothetical attack on the power infrastructure and grid networks of a country could significantly hinder a country's functioning. Disruptions to power grids and critical infrastructure means patients in hospitals dependent on critical care may suddenly find themselves vulnerable, banking infrastructure could go offline, there could be fatal accidents involving transportation infrastructure with flight and train communication and navigation being targeted, citizen data could be ex-filtrated, etc. This has led governments to shift to multi-stakeholder whole-of-society approaches to bridge the traditionally demarcated civil military gaps (Prince 2021).

Cyber-Peacekeeping: Potential and Stasis

In contrast to cyberwar, cyber-peacekeeping remains relatively less explored with states seeking to secure their sovereignty prior to contemplating collaboration. Researchers began examining cyber peacekeeping in the early 2000s with studies such as that of Cahill and colleagues recommending the application of UN Peacekeeping principles to Cyberspace (Cahill et.al. 2003). Despite this initial interest, cyber peacekeeping remained a sporadically explored if not altogether underexplored area of research given the sovereignty concerns worldwide. In view of the proliferation of cyber modalities across every aspect of life, coupled with an environment of geostrategic competition, most states would argue that we are in a state of cyber competition and at worst a state of crisis as seen by current conflicts and the vulnerability of CIIs and supply chains globally.

The lack of active cyber peacekeeping does not mean that cyber means are not being used during peacekeeping operations. As mentioned in the section above cyber technologies are intrinsic to most operational capabilities, realistically, therefore, they are already being used as operational support for peacekeeping operations. However, if pursued in a structured manner there are significant areas where states could come together to adapt collaborative cyber efforts to existing peacekeeping norms. For instance, Robinson and his colleagues examined the value of cyber peacekeeping and how such efforts could significantly enhance traditional peacekeeping efforts (Robinson et al. 2019). In 2020, Ahmed Almutawa examined the value of establishing a UN Cyber peacekeeping team and the need to define its legal status (Almutawa 2020).

While peacekeeping efforts have been *'cyberized'* in terms of their operational reality, as mentioned in the previous section, the threat matrix is becoming increasingly complicated with the blurring of the lines between civilians and combatants. On the one hand, conflict spaces are witnessing the rise of digital defenders and civilian hacktivists. However, there also has been a rise of malicious intent hacktivism with state sponsored and vigilante type groups taking sides in conflict, exacerbating targeted violence and attempting to degrade citizen morale and infrastructure. Vulnerable populations are also dealing with increases in cybercrime and extortion.

In addition, there are spaces where cyber proliferation is high but digital redundancy (in terms of the ability for physical infrastructure to survive attack) and digital literacy are incredibly low. The most vulnerable groups in these spaces are subject to cyber violence and physical violence that cannot be reported due to intentional degradation of the information infrastructure.

Theoretically, in pre-conflict stages, cyber peacekeeping could be used as a means to bolster weak states' abilities to defend critical infrastructure while also keeping an eye out for hate speech against targeted groups and minorities. Given the objectivity of peacekeepers and the lack of incentive to intervene, attribution would not be the primary goal of the operational support, but prevention of harm and limitation of violence would be the primary aim. In active conflicts where the consent of both state parties exists, peacekeepers could work towards limiting collateral damage to the extent possible through monitoring of networks and provision of support in case of degradation of infrastructure.

Additionally, the rise of threats from EDTs such as drones, AI, biotechnology, etc. would all require a structured organizational approach. It is not enough to just use cyber operations in traditional peacekeeping, there is a need to engage with it systematically to counter existing and future threats in a transparent and reliable manner. This would require systematic engagement by member states who provide peacekeeping forces to undertake efforts to build digital literacy and up skill their workforces. Disinformation could be used to target at risk populations, obscure crisis communication, and deepfakes could be used to humiliate vulnerable genders and children while also targeting and doxing[3] them enabling physical violence against them.

Furthermore, if the cyber-attack is devastating, and is accompanied by more conventional attacks, then the chaos of warfare is further compounded by the denial of information to citizens. For instance, citizens may lose access to vital, life-saving information at such a critical time owing to a cyber-attack. What further complicates the picture is that in some contexts states themselves block citizen access to cyber infrastructure, as has been the case with the Indian government's protracted internet shut downs in conflict affected areas such as Kashmir and Manipur (Rajvanshi 2023). There is a need to operationalize a strong legal framework that treats cyber infrastructure as a part of basic services which every citizen is entitled to, in order to prevent arbitrary misuse and manipulation by states. It is keeping these circumstances in mind that experts and researchers working on cyber warfare have recommended that international organizations such as the United Nations take cyber peacekeeping more seriously.

Digital Blue Helmets, launched in 2016, was arguably the first measure to adopt cyberspace, but the initiative still has not garnered the amount of attention that it needs (Akatyev and James 2017). Given the interconnected nature of Critical International Infrastructure and interdependence in

[3] Doxing is the act of revealing identifying information about someone online, such as their real name, home address, workplace, phone, financial, and other personal information.

terms of supply chains, these efforts could look to existing regional and international alliances and mechanisms that undertake collaborative efforts towards capacity building in cyberspace. For instance, the Association of Southeast Asian Nations (ASEAN) recently developed the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), with an aim to bolster cybersecurity capacity through training and workshops.

Gendering the Cyber Domain

While efforts to establish or bolster cyber peacekeeping as a practice have been limited to say the least, the changing security environment could lead to a shift in thinking for states that seek to ensure defensive partnerships in the cyber domain while pursuing responsible and transparent offensive capabilities. It is unlikely that states will move back from active engagements in cyberspace but perhaps transparency regarding the operations could go a long way towards fostering trust and building partnerships. The current prognosis is bleak, however, given the digital divide with a majority of critical infrastructure being operated from the West leading to insecurity amongst South and Southeast Asian nations who cannot count on Big Tech generosity in their own crises. Additionally, the rise of populism and authoritarianism across the globe has meant that the proliferation of norms regarding cyber governance have also suffered a setback with more states seeking to pursue cyber sovereignty rather than cyber solidarity.

Within this overall bleak situation, a promising solidarity intervention is the gendered initiative of the Women in International Security and Cyberspace (WIC) Fellowship which aims to address the need for a greater proportion of representation from women diplomats at the United Nations negotiations concerning cyberspace. Jointly organized and sponsored by the governments of Australia, Canada, the Netherlands, New Zealand, the United Kingdom and the United States, WIC program seeks to develop cyber governance capacities of the Fellows for their participation in the male dominated UN First and Third Committee which deal with arms control and disarmament processes (GFCE/WIC 2024).

Another potential area of cooperation could be the protection of vulnerable gender identities across cyber and physical spaces. Cyber tools like AI are dual edged technologies and often the problem and the solution surrounding their misuse may emerge from the same source. Potential collaboration towards safeguarding vulnerable gender identities, however, requires an honest examination of the risks they face at present. Historically, during times of war, women have often been the targets of physical and sexual violence, with enemy soldiers often using rape as a tool to ‘demean’ and ‘dishonor’ the adversary (Enloe 2014). There are valid fears that these forms of violence could translate into the cyber domain as well. The rapid progress made by AI, especially in the visual sphere has meant that fake images and videos created to demean an adversary’s women can be used as a tool of psychological warfare.

The loss of information access in times of conflict can significantly increase threat to life and a targeting of minorities and vulnerable populations. Furthermore, disinformation and mal-information campaigns coupled with surveillance and targeting are also ways in which vulnerable populations, including women, can be caught in the cyber crossfire. If a cyber-peacekeeping force is to be established there would need to be sustained efforts aimed at incorporating gender within the discourse at a foundational level rather than something to be tacked on later as an afterthought. For example, countries that volunteer peacekeepers for such missions would need to train digitally literate forces (inclusive of female, non-binary, and other identities) and ensure the heterogeneity of the force composition. At national levels, therefore, there would need to be sustained efforts towards first up skilling citizenry by establishing cyber commands and organizations from whom volunteer peacekeepers could be sent.

Secondly, it is not enough to train digitally literate forces on a technical level but there would be a need to educate them and build social and cognitive resilience given the high levels of AI sophistication and the dangers of buying into misinformation in times of crisis. Through the establishment of cyber commands and joint exercises, countries would need to build social resilience and train their citizenry to better parse through the large swathes of information being proliferated today. Efforts like Singapore’s ‘Total Defense’ or Digital Literacy Initiatives could go a long way towards capacity building through whole-of-society efforts. Canada and the Netherlands also launched the ‘Global Declaration on Information Integrity’ online initiative which was signed by 30 other countries in 2023. The WIC initiative has been mentioned above. However, all these countries belong to the Global North and there is a need to reassess if such efforts will be replicated in the Global South as well. The information landscape in the global south is fraught to say the least.

A lack of redundancy and critical infrastructure protection within conflict regions will also remain a major concern and cyber peacekeepers would also need to be trained in infrastructural rebuilding, rapid response, and crisis communication to be able to assist regions and people where digital proliferation may be prevalent and weaponized. Additionally, there would need to be a system of checks and balances regarding the structural proliferation of cyber peacekeepers and cyber tools in a responsible manner to prevent the failures of traditional peacekeeping. The conduct of peacekeepers and the correlation of peacekeeper presence and increase in sex trafficking have been issues of grave concern. A paper in 2018 found that an increase in the presence of peacekeeping forces has been accompanied by an increase in the probability that the host state is a destination for sex trafficking (Bell et al 2018). The paper found that while the presence of peacekeepers helped reduce conflict it added to the complications of post conflict environments. Consequently, a priority concern has to be ensuring the potential anonymity of cyber means to prevent misuse for malicious purposes like sex trafficking and other forms of abuse and sexual misconduct.

Dual Edged Tools: Surveillance as Weapons and Shields

Having looked at the structural integration of possible cyber peacekeeping bodies with the discourse on gender, this section will look at surveillance and monitoring as double-edged swords for cyber peacekeeping. A significant aspect of cyber-peacekeeping that researchers recommend is the use of cyber tools such as unmanned drones for Intelligence, Surveillance and Reconnaissance (ISR) as well as Observation, Monitoring and Reporting (OMR) purposes. Like with all other tools, drones and other unmanned autonomous vehicles are inherently dual use. In the hands of responsible civilians and state actors they can be used to monitor Critical Infrastructure in conflict regions and ensure connectivity in times of great crisis while also providing information on impending strikes and dangers. However, in the hands of state sponsored proxies or independent actors, there are significant concerns regarding the use of such technologies for surveillance and monitoring of vulnerable and targeted groups. In the hands of malicious actors, these tools could be used to *dox* and target vulnerable sections of society leading to increased outbreaks of violence. They could also be used to generate deepfakes and spread disinformation in times of crisis, thus completely eroding trust in government and reinforcing pre-existing cleavages in societies.

The vulnerability of women and children in cyberspace mirrors their vulnerability in real life, particularly in conflict spaces. In 2023, the UN Secretary General’s 14th report stated that between January 2022 – December 2022, there had been 2,455 cases of CRSV (UNSG 2023). Women and girls accounted for over 94 percent or 2,297 of these reported cases. There is a need to be mindful of these power dynamics and emphasize the importance of safeguarding vulnerable populations by avoiding the creation of alternate avenues of exploitation instead. Apart from vulnerability during conflict, there are also other gendered considerations that are important to keep in mind here, and these pertain to the following –ISR and OMR. Here, the issue of ‘unmanned’ technology and its inherent biases comes into play. However, before we discuss these issues in detail, a theoretical understanding of these ‘spaces’ must be provided.

Activities such as ISR and OMR are not a part of direct warfare but are often seen as auxiliary practices. Thus, as opposed to the traditional imagination of the battlefield, i.e. that of male soldiers of rival groups fighting each other (under the Geneva Convention: laws of war), ISR & OMR spaces are firstly imagined as operating under a veil, away from the zone of the conflict. They are also seen as being highly influenced by technology, which tends to mean that those protocols and codes derived from the laws of war that impact direct (as opposed to virtual) warfare are often held in abeyance. The relative impunity enjoyed by ISR and OMR operators can also result in a problematic gaze towards women in the conflict zone, where surveillance technologies can be used for control, and possibly, infringement of the privacy and sexuality of women stuck in conflict zones. Given the problematic history of sexual abuse by military forces engaged in conflict, the role of cyber technology and its deployment by malicious actors in an anonymized manner only increases the impunity with which these parties can operate.

Conflict zone populations that are under surveillance may also feel impotent and ‘demasculinized’ owing to the bio-politics of peacekeeping (Tripathy 2014). As Manjikiani (2014) argues, technology is often seen as dehumanized, and thus, being controlled by surveillance technologies can also lead to the people in conflict zones feeling alienated as well as disempowered, as they are controlled by an impersonal and opaque force. Also, through the distance and ‘remote control’ that cybertools create, peacekeeping forces can fall under the impression that they are ‘above’ accountability (Ahmed 2011). Furthermore, conflict zone populations are rarely empowered enough to demand transparency, and control over the information that is extracted and shared by peacekeeping forces. Thus, the chances of abuse and misuse heighten if cyber ethics and norms regarding peacekeeping are not instituted and enforced in the conflict zone.

Queered Spaces, Fetish, and Masculinist Intervention

While Mary Manjikiani uses the perspective of queerness to investigate the world of espionage, the power differential may also result in a ‘queering’ of the native population in conflict zones (Manjikian 2020). As discussed earlier, heteronormative assumptions are rife in the conflict zone, with the protectors (peacekeeping forces) imagining themselves as cis-men, and the population as either female, or queer with the assumption that power lies in a heterosexual masculinity (Rao 2020). These biases may also make their way into algorithmic assessments of conflict situations prior to rescue operations, essentially determining who is worthy of being ‘saved’. While information gathering and on ground analysis may be automated, developing a cyberliterate peacekeeping force capable of understanding, parsing, and interpreting information in a rapid and efficient manner would require systematic investment in a cyber peacekeeping force. Open-Source Intelligence (OSINT) and Human Intelligence (HUMINT) would need to be aligned to ensure that one is not sacrificed for the other.

Additionally, the barrier of digital literacy for women in traditionally patriarchal societies would also need to be overcome within a cyber-peacekeepers space as well as a conflict region space. The unequal access to technology in highly patriarchal societies, where women are not trusted with devices such as mobile phones because of fears that they can be led astray, remains a significant concern. There is another harmful consequence of this. Unequal access to technology also means that women may have lesser access to crucial information during conflict and disasters.

Another aspect of gender that needs to be considered in cyber-peacekeeping is the intersection of gender and ethnicity. In various conflicts, women belonging to certain ethnicities are marked as threats. For instance, the securitization of the *hijab* in cyber-discourse paints Arab and Muslim women in two ways. The first portrayal is that of the dangerous other, whose ‘threat’ is doubly amplified because of her veil and its ability to hide. This gets reflected in other forms of popular discourse, such as in Hollywood films, where Arab or oriental backwardness is depicted through the veiling of women (Akabli and Chahdi 2022). This also means that in visual regimes engineered by technologies such as drones, the images of veiled women can evoke the perception of threat and backwardness, which undermines the ability of those 'surveying' to treat their subjects as fully human and agential. Another manner in which gender and ethnicity are instrumentalized is through fetishization and 'degradation pornography', in which women of certain ethnicities are fetishized through the 'veil', and then portrayed as occupying an inferior position and being sexual dominated by (mostly) white men (Smith and Luykx 2017). This race-play is not just restricted to Islamic or Arab cultures, Asian women too are subjected to this hyper-sexual and dominant gaze, which also results in the complementary de-masculinization of men from these countries (Matsumoto 2020). Given AI's ability to produce deepfakes, and also to proliferate them on a large scale, revenge-porn can potentially be used in conflict zones to morally disempower vulnerable communities.

Conclusion

Cyber-peacekeeping provides significant potential for reframing how cyber tools are used, securitized and proliferated. There are concerns that cyber peacekeeping might just replicate and mimic traditional peacekeeping practices which have been accused of producing their own ontological violence. Building a cyber-peacekeeping force at an international level, however, requires significant investment in digital literacy and up skilling at the national level by nation states. Considerations of gender vulnerability for adults and children need to be integrated at each step of the digitization process. Engendering digital technologies is a key aspect of significant global governance initiatives on cyber technologies and AI. Additionally, for women to be participatory agents in this up skilling, there is a need for governments to incentivize female participation in STEM spaces which is difficult to encourage in traditionally patriarchal and masculinist societies. While there are ongoing efforts towards building digital self-reliance in countries in South and Southeast Asia, the overall global digital divide remains significantly large.

This paper has attempted to provide a brief overview of the shifting digital landscape and the need for a reorientation in our approach to security and technology in the context of cyberspace and peacekeeping. Cyber tools and digital integration are only going to increase significantly over the next few years and in its current state, peacekeeping as a practice runs the risk of remaining ineffective at best and deleterious at worst in cyberspace. The need to build digital capacity in countries that provide peacekeepers, and to include more women and queer identities in peacekeeping spaces - both physical and digital - remains an ongoing struggle. Lessons from conflicts in Ukraine and Gaza show us that while traditionally masculinist military violence has adopted digital forms, the inherent gendered nature of its destructive potential remains unchanged. To counter that, there needs to be a conscious effort to build an inclusive in composition and pluralistic in deployment force capable of countering misogyny and its violence in the cyber and physical realm. In the absence of such sustained efforts, we are doomed to repeat the failures of physical peacekeeping in the digital realm as well.

References

Ahmed, Manan. 2011. “Adam’s Mirror: The Frontier in the Imperial Imagination.” *Economic and Political Weekly*. 46 (13) March 25, 2011: 60–65. https://www.epw.in/journal/2011/13/reflections-empire-special-issues-specials/adams-mirror-frontier-imperial.

Akabli, Jamal, and Chadi Chahdi. 2022. “Hollywood’s (Mis) Construction of Gender: The Aesthetics and Politics of Stigmatising Arab/Muslim Women.” *International Journal of Linguistics, Literature and Translation* 5 (8): 17–28. https://dx.doi.org/10.32996/ijllt.2022.5.8.3.

Akatyev, Nikolay, and Joshua James. 2017. “United Nations Digital Blue Helmets as a Starting Point for Cyber Peacekeeping.” In *European Conference on Cyber Warfare and Security*, 8–16. Academic Conferences International Limited. https://www.researchgate.net/publication/321069756_United_Nations_Digital_Blue_Helmets_as_a_Starting_Point_for_Cyber_Peacekeeping.

Almutawa, Ahmed. 2020. “Designing the Organisational Structure of the UN Cyber Peacekeeping Team.” *Journal of Conflict and Security Law* 25 (1): 117–47. https://doi.org/10.1093/jcsl/krz024.

Bell, Sam, Flynn.E, Michael, Machain, Martinez Carla. 2018. “UN Peacekeeping Forces and the Demand for Sex Trafficking.” *International Studies Quarterly* 62 (3): 643–55. http://dx.doi.org/10.1093/isq/sqy017.

Bellaby, Ross W. 2023. “Political Autonomy, the Arab Spring and Anonymous.” In *The Ethics of Hacking*, 53–72. Bristol University Press. https://bristoluniversitypressdigital.com/monochap/book/9781529231847/ch003.xml.

Brown, Deborah, and Allison Pytlak. 2020. “Why Gender Matters in International Cyber Security”. *Association for Progressive Communications*. April 21, 2020. https://www.apc.org/en/pubs/why-gender-matters-international-cyber-security.

Caballero-Anthony, Mely and Alistair Cook. eds. 2013. *Non-Traditional Security in Asia: Issues, Challenges and Framework for Action*. Singapore: ISEAS Publishing.

Cahill, Thomas, K. Rozinov, C. Mule. 2003. “Cyber Warfare Peacekeeping.” In *IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, 2003.*, 100–106. IEEE. https://ieeexplore.ieee.org/abstract/document/1232407/.

Consortium on Gender, Security, and Human Rights. 2010. “Masculinities and Peacekeeping”. https://genderandsecurity.org/sites/default/files/masculinities_and_peacekeeping_literature_review_0.pdf.

Dadas, Caroline. 2020. “Making Sense of #MeToo: Intersectionality and Contemporary Feminism – CFSHRC.” https://cfshrc.org/article/making-sense-of-metoo-intersectionality-and-contemporary-feminism/.

Day, Adam. 2020. “The Future of UN Peace Operations in a Changing Conflict Environment.” *UN DPO Future of Peace Operations Project*. https://peacekeeping.un.org/sites/default/files/future_of_peacekeeping_operations_in_a_changing_conflict_environment.pdf.

Digital Forensic Research Lab. 2024. “Undermining Ukraine: How Russia Widened its Global Information War in 2023 - Atlantic Council.” Atlantic Council. February 29. https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/.

Enloe, Cynthia. 2014. *Bananas, Beaches and Bases: Making Feminist Sense of International Politics*. Univ of California Press.

Erkanli, Sertan. 2023. “Unmanned Eyes in the Sky: The Evolution and Impact of ISR Drones and UAVs ". *Defensebridge*. May 3, 2023 https://defensebridge.com/article/unmanned-eyes-in-the-sky-the-evolution-and-impact-of-isr-drones-and-uavs.html.

Fischerkeller, Michael, and Richard J. Harknett. 2019. “Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation.” *The Cyber Defense Review*: 267–87. https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf.

GFCE/WIC. 2024. “Women in International Security and Cyberspace (WIC) Fellowship.” https://thegfce.org/project/women-in-international-security-and-cyberspace-fellowship/Harding.

Luke Dan Sabbagh, and Isabel Koshiw. 2022. “Russia Targets Ukraine Energy and Water Infrastructure in Missile Attacks Ukraine” *The Guardian*. October 31, 2022. https://www.theguardian.com/world/2022/oct/31/russian-missiles-kyiv-ukraine-cities.

Giannaros, Anastasios, et.al. 2023. “Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions.” *Journal of Cybersecurity and Privacy* 3 (3): 493–543. https://doi.org/10.3390/jcp3030025.

Guzman, Chad de. 2022. “Meta’s Facebook Algorithms ‘Proactively’ Promoted Violence Against the Rohingya, New Amnesty International Report Asserts.” *Time*, September 28, 2022. https://time.com/6217730/myanmar-meta-rohingya-facebook/.

Hirblinger, Andreas, Julie Marie Hansen, Kristian Hoelscher, Åshild Kolås, Kristoffer Lidén and Bruno Oliveira Martins. 2023. “Digital Peacebuilding: A Framework for Critical–Reflexive Engagement.” *International Studies Perspectives* 24 (3): 265–84. https://doi.org/10.1093/isp/ekac015.

Jessica Brandt. 2023. “Propaganda, Foreign Interference, and Generative AI”. Brookings, November 8, 2023.https://www.brookings.edu/articles/propaganda-foreign-interference-and-generative-ai/.

Maad, Assma, Samuel Forey, and William Audureau. 2024. '40 Beheaded Babies’: Deconstructing the Rumor at the Heart of the Information Battle between Israel and Hamas.” *Le Monde*, March 4, 2024. https://www.lemonde.fr/en/les-decodeurs/article/2024/04/03/40-beheaded-babies-the-itinerary-of-a-rumor-at-the-heart-of-the-information-battle-between-israel-and-hamas_6667274_8.html.

Mackinnon, Amy and Rishi Iyengar. 2022. “Whatever Happened to Russia’s Vaunted Cyberoffensive?” December 16, 2022. https://foreignpolicy.com/2022/12/16/russia-cyberoffensive-cyberattack-war-ukraine-putin/.

Manjikian, Mary. 2014. “Becoming Unmanned: The Gendering of Lethal Autonomous Warfare Technology.” *International Feminist Journal of Politics* 16 (1): 48–65. https://doi.org/10.1080/14616742.2012.746429.

———. 2020. *Queerness, Secrecy, and Revelation*. Gender, Sexuality, and Intelligence Studies. https://doi.org/10.1007/978-3-030-39894-1_5.

Matsumoto, Kendall. 2020. “Orientalism and the Legacy of Racialized Sexism: Disparate Representational Images of Asian and Eurasian Women in American Culture.” *Young Scholars in Writing* 17: 114–26. https://youngscholarsinwriting.org/index.php/ysiw/article/view/305.

Murphy, Matt. 2010. “War in the Fifth Domain.” *The Economist*, July 1, 2010.

https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.

Prince, Conrad. 2021. "The UK Government's New Cyber Strategy: A Whole of Society Response." December 15, 2021. https://www.rusi.org/explore-our-research/publications/commentary/uk-governments-new-cyber-strategy-whole-society-response.

Qiao-Franco, Guangyu. 2024. "An Emergent Community of Cyber Sovereignty: The Reproduction of Boundaries?" *Global Studies Quarterly* 4 (1). https://doi.org/10.1093/isagsq/ksad077.

Rajvanshi, Astha. 2023. "How Internet Shutdowns Wreak Havoc in India." *Time*, August 15, 2023. https://time.com/6304719/india-internet-shutdowns-manipur/.

Rao, Rahul. 2020. *Out of Time: The Queer Politics of Postcoloniality*. Oxford University Press.

Robinson, Michael, Kevin Jones, Helge Janicke, Leandros Maglaras. 2019."Developing Cyber Peacekeeping: Observation, Monitoring and Reporting." *Government Information Quarterly* 36 (2): 276–93. https://doi.org/10.1016/j.giq.2018.12.001.

Sharma, Divyam. 2024. "Explained: How Emergence Of 'Disruptive Technology' Is Transforming Modern Wars." NDTV.Com. March 10, 2024 https://www.ndtv.com/india-news/explained-how-emergence-of-disruptive-technology-transforming-modern-wars-5210754.

Tripathy, Jyotirmaya. 2014. "Biopolitics, Torture, and the Making of the Terrorist: An Essay on Un-Moderning." *Social Semiotics* 24 (2): 159–74. https://doi.org/10.1080/10350330.2013.851456.

Ullah, Faheem,Edwards, Matthew,Ramdhani, Rajiv, Chitchyan, Ruzanna, Babar,Ali M, Awais Rashid. "Data Exfiltration: A Review of External Attack Vectors and Countermeasures." *Journal of Network and Computer Applications* 101: 18–54. https://doi.org/10.1016/j.jnca.2017.10.016.

UN Peacekeeping. 2024. "DATA." United Nations Peacekeeping. January 31, 2024. https://peacekeeping.un.org/en/data.

UN SG Report. 2023. "14th Report of the United Nations Secretary General on Conflict Related Sexual Violence." https://www.un.org/sexualviolenceinconflict/wp-content/uploads/2023/07/SG-REPORT-2023SPREAD-1.pdf.

UN Women. 2000. "UN Security Council Resolution 1325 on Women Peace and Security. https://www.unwomen.org/en/docs/2000/10/un-security-council-resolution-1325.