WE
Vol 5 No. 2
December 2024
e-ISSN: 2583-2298

ANALYSING THE FRAMEWORK FOR RESPONSIBLE CYBER ACTIVITIES THROUGH A GENDER LENS

PULOMA PAL*

ABSTRACT

Eleven voluntary and non-binding principles are established by the Framework of Responsible State Behaviour in Cyberspace, which was unanimously accepted by the UN General Assembly in 2015 to regulate state behaviour in the digital sphere. Nonetheless, the conversation around adopting these standards has paid little attention to their gendered aspects and consequences. This essay explores how gender concerns may be successfully mainstreamed into the day-to-day implementation of the norms by providing a thorough gender analysis of the framework. The research explores the crucial need for gender-sensitive capacity development programmes to enable governments to implement their responsibilities under the framework, drawing on experiences and viewpoints from Latin America and the Caribbean. To ensure that initiatives supporting responsible state behaviour in cyberspace align with and strengthen larger commitments to gender justice, it also emphasises the significance of creating explicit connections within cybersecurity frameworks and current gender equality goals. The article also emphasises the importance of guaranteeing that women and gender minorities have significant leadership roles in cybersecurity governance procedures at all levels. The framework will only fully represent the needs and experiences of all stakeholders if a variety of voices and viewpoints are included. The article concludes with a list of doable suggestions for promoting gender issues in the Framework of Responsible State Behaviour in Cyberspace implementation. These may include, creating a thorough gender and cybersecurity toolbox. This would help assist the stakeholders in incorporating gender viewpoints into their work and setting up specific funding sources, to support efforts aimed at, developing the capacity for a gender-responsive approach.

Keywords: *Women, Gender Equality, Cyberspace.*

1. INTRODUCTION

The idea of a Responsible State Behaviour in Cyberspace is largely influencing the global Cybersecurity norms and laws. Nonetheless, to guarantee this framework's efficacy and inclusion, a thorough gender analysis is necessary. Within the allotted word count, this essay seeks to investigate the gender aspects of this significant subject by offering a careful and accessible analysis. The framework addresses important concerns including international collaboration, capacity building, and conflict avoidance. It lays forth fundamental principles, rules, and standards for responsible state action in cyberspace. Nevertheless, it is vital to take into account how gender interacts with these different elements to fully realise the framework's potential. To do this, it is necessary to look at how different gender identities were represented and included in the framework's creation and application. It is also necessary to comprehend how cyber threats affect different genders and the particular cybersecurity difficulties that marginalised communities confront. The framework's inclusion of a gender-responsive strategy has the potential to enhance the global cybersecurity environment by making it more equitable, inclusive, and productive. The present introduction lays the groundwork for an in-depth examination of the gender-related factors, obstacles, and prospects within the context of Responsible State Behaviour in Cyberspace.

2. FRAMEWORK OF RESPONSIBILITIES OF STATE BEHAVIOUR IN CYBERSPACE

The Open-Ended Working Group (OEWG) and the United Nations Group of Governmental Experts (GGE) developed the framework of responsible state behaviour in cyberspace, which outlines important norms, principles, and guidelines to promote stability and security in states' use of information and communication technologies (ICTs) (CyberPeace Institute, 2024). A significant advancement in the development of global cybersecurity within a rules-based framework has been made by this consensus accord, which is now politically obligatory for all UN members. (FDFA, 2021) (Lewis, 2022).

*Amity University, Noida, Email: puloma001.pal@gmail.com

©WE-Faculty of Arts

Four pillars support the framework: principles and standards for responsible state behaviour, voluntary non-binding norms, international law, and methods to foster confidence. Eleven specific norms are included in it, all of which are intended to prevent or lessen the negative effects of cyber incidents. (FDFA, 2021). These include working together to develop security and stability measures, taking relevant information into account when responding to incidents involving ICT, and taking reasonable steps to ensure the integrity of the supply chain. (Hogeveen, 2022). This paradigm is essential for creating a consensus on what constitutes appropriate state behaviour and encouraging responsibility in the face of expanding cyber threats and difficulties. In the digital era, the framework can preserve human rights, defend vital infrastructure, and promote international peace and security by offering a common basis for responsible behaviour. (Lewis, 2022).

Nonetheless, the sheer presence of established standards does not guarantee their observance and provide stability in cyberspace. It is imperative to formulate a joint diplomatic approach aimed at enhancing the enforcement of rules and augmenting responsibility in cases when they are disregarded. This entails establishing guidelines for group activity, deciding on attribution criteria, and enforcing just, legitimate, and efficient penalties for infractions. The framework has the potential to facilitate the gap between the discourse and reality of responsible state behaviour in cyberspace using international collaboration, building capacity, and public-private partnerships. (Broeders, Delerue, & Sukumar, 2023). This framework offers a basis for supporting security, stability, and transparency in the digital realm as the world community continues to negotiate the difficulties provided by evolving technologies.

3. THE DIMENSIONS OF GENDER OF THE RESPONSIBLE STATE BEHAVIOUR FRAMEWORK IN CYBERSPACE

3.1 Participation and Representation

The responsible state behaviour structure in cybersecurity would require to include and empower women and gender minorities in decision-making procedures. This field has been historically male-dominated. With women and other gender identities, under-represented in leadership roles and policy discussions (Miller, Shires, & Tropina, 2021). This can be achieved through targeted capacity-building initiatives, mentorship programmes, and the creation of an inclusive space for diverse voices across the globe. (UNIDIR, 2021). In addition to posing a unique barrier to accessing digital technology and resources, cyberspace threats and assaults frequently have a disproportionately negative impact on women and disadvantaged groups, which can result in cyber-enabled gender-based violence, online harassment, and stalking. This happens due to the socio-economic and cultural barriers, these groups face. The framework must acknowledge such gendered impacts. Prioritise the targeted policies and interventions to address them.

3.2 Effects of Cyberspace on Gender

Cyberspace threats and assaults frequently disproportionately affect women and other groups that are marginalised. (Miller, Shires, & Tropina, 2021). The Gender-based violence that is enabled by technology. Here we can put examples of non-consensual sharing of private photos, online bullying, stalking etc. Such incidences may have serious and negative impacts on the victim's social, professional, and psychological well-being. (Miller, Shires, & Tropina, 2021). Furthermore, because of socioeconomic and cultural limitations, women and gender minorities may have particular difficulties in using digital technology and services. The framework for responsible state conduct has to take note of these gendered effects and give top priority to the creation of focused policies and initiatives to deal with them.

3.3 Inclusive Capacity Building

Programmes for capacity-building and training should be created with an inclusive and gender-responsive approach to support gender balance and strengthen women and underrepresented groups in the cybersecurity field. This entails including women and gender minorities in projects aimed at enhancing their ability, delivering training on unconscious prejudice, conducting gender sensitivity, and incorporating training on gender equality into all organisational procedures (EIGE,

© WE - Faculty of Arts

n.d.). To prevent unconscious gender bias from influencing decision-making and selection procedures in the cybersecurity industry, this will assist in identifying obstacles and putting into practice suitable gender-informed measures (GAFCC).

3.4 Gendered Threat Assessments

To effectively handle the distinct vulnerabilities and hazards that various gender identities experience in cyberspace, gender-specific factors must be incorporated into threat assessments and risk evaluations. The gender-specific considerations are required to integrate into the threat assessment and evaluation of risk to address the unique vulnerabilities and hazards that people with different gender identities (like males) encounter in Cyber security (UN Women, 2024). Hence, developing tailored cybersecurity strategies, collecting and analysing the gender-disaggregated data on cyber threats, involving women and gender minorities in threat assessment processes, and acknowledging women and marginalised groups are disproportionately affected by cyber threats, are all essential in addressing such problems.

4. CHALLENGES AND OBSTACLES IN THE FIELD OF CYBERSPACE.

Despite various advancements, gender discrimination and stereotypes are still existing the sector of Cybersecurity. It might be difficult for women in cybersecurity to be taken meticulously by their male colleagues and to overcome doubts about their technological prowess. Negative preconceptions can result in discrimination in employment, work assignments, and career progression. Examples of these stereotypes include the idea that women don't have a *"hacker mindset"* or are less competent in technical professions. (Offenso Hackers Academy, 2023).

It is critical to support hiring procedures that prioritise credentials and merit above gender to combat these prejudices. Employees who get unconscious bias training may become more cognizant of how preconceived notions and deeply held beliefs may affect judgment. (Offenso Hackers Academy, 2023). Driving good change also requires cultivating an inclusive and transparent culture where workers feel comfortable bringing up challenges linked to bias. Because of social norms around caring responsibilities, women may be disproportionately affected by the high pressure and long hours of cybersecurity. Such problems can further lead it to harder maintain a balance in work and life. Companies may assist in overcoming such obstacles by providing flexible work schedules, family-friendly policies, and an understanding of the need of work-life balance for preserving workers' well-being and output. Unfortunately, there are fewer advisors for prospective female workers in cybersecurity since there are fewer women in cybersecurity professions. In an industry where women are underrepresented, the absence of strong female role models may be extremely discouraging. (LEARN.ORG, 2024). There are fewer inspirations for women because males make up the bulk of well-known leaders and success stories. Because there aren't many women in senior roles, it can be difficult for women to perceive a career path in cybersecurity, which could lower their self-confidence and goals. (WomenTech Network, 2024). The absence of supervisors who are cognizant of the unique challenges faced by women might impede their professional growth.

5. THE GENDER DIGITAL DIVIDE AND PROMOTING THE GENDER EQUALITY

The term “Gender Digital Gap”, refers to the variations in men and women who can access to as well as the use of digital technologies. The number of women who work in Cybersecurity is usually affected by this Gender Gap. Women may encounter difficulties getting access to STEM education and training options. This hindrance may create difficulties and challenges to their ability to enter the cybersecurity industry. This is especially true for women who belong to the marginalised groups. To resolve such issues, we would require a multifaceted strategy to address the gender digital divide. This may include putting money into initiatives that teach girls and women digital literacy to improve their exposure to and familiarity with technology. Also, encouraging young women to pursue STEM education and careers to spark their curiosity in cybersecurity. To quote an example here, the article from India today states a steady rise in women’s interest in STEM courses in India. The article talks about the reports and surveys. It talks about the current enrolment of women in STEM degrees compared to males is

© WE - Faculty of Arts

45:55. The article, however, mentions that the ratio is still low as compared to men. Between the years 2022 to 2024, the participation of women in STEM degrees has significantly risen to 12% (India Today, 2024). Apart from this, facilitates the professional growth of women in the sector by offering them networking and mentoring opportunities.

The framework for responsible state behaviour in cyberspace offers a chance to advance inclusion and gender equality in the digital sphere. Through the integration of gender-responsive methodologies in the establishment and execution of standards and directives, the global community may guarantee that the distinct obstacles and viewpoints of women and marginalised communities are suitably attended to. This may comprise ensuring that women and other gender identities are equally represented in framework-related decision-making processes. (WomenTech Network, 2024). Performing the threat assessments tailored to a certain gender to comprehend how cyber risks disproportionately affect women and other marginalised groups. Also, creating a customised cybersecurity plan that would address the unique requirements and weaknesses of various gender identities

6. THE BOTTOM LINE

To achieve Gender parity in Cybersecurity, the public sector, the commercial sector and the government must work together. The Government may play a critical role in the development and implementation of policies that promote diversity and inclusion in the cybersecurity industry. (Cyber Defense, 2023). Civil society groups possess the capability to advance women's rights and heighten the consciousness of discrimination against women across all domains. The business sector may set a benchmark by enacting policies that are inclusive when it comes to recruiting and promoting employees, offering mentoring and training programmes that are sensitive to gender, and assisting female-led cybersecurity efforts. Together, we may tackle the gender digital gap, dismantle gender prejudices, and make use of the framework for responsible state behaviour to build a more varied, just, and safe online space for all. (WomenTech Network, 2024).

The Responsible State Behaviour in Cyberspace framework is a global cybersecurity standard that promotes stability and security in states' use of information and communication technologies (ICTs). It consists of eleven specific norms designed to prevent or lessen the negative effects of cyber incidents. However, the framework does not guarantee their observance and requires a joint diplomatic approach to enhance enforcement. Gender dimensions within the framework include participation and representation, effects of cyberspace on gender, inclusive capacity-building, and gender-specific threat assessments. Empowering women and gender minorities in decision-making procedures, addressing the disproportionate effects of cyberspace threats, and addressing gender-enabled violence, online harassment, and stalking are essential steps. The Programmes for inclusive capacity building and training should be developed to promote Gender parity and bolster the status of women and other underrepresented groups in the cybersecurity industry.

In the cybersecurity industry, gender prejudice and stereotypes still affect women's perceptions of their technological ability and the likelihood of discrimination in hiring, work assignments and career progression. A business that understands the need for work-life balance and provides flexible scheduling and family-friendly practices can help. To address the Gender Digital divide, funding must go towards initiatives that teach girls and women digital literacy, encourage young women to pursue careers in STEM, and foster professional growth via networking and mentorship.

REFERENCES

Broeders, D., Delerue, F., & Sukumar, A. (2023, June 29). *EU Cyber Direct*. Retrieved May 15, 2024, from eucyberdirect.EU: https://eucyberdirect.eu/research/responsible-behaviour-in-cyberspace

Cyber Defense. (2023, March 07). *Cyber Defense*. Retrieved May 21, 2024, from orangecyberdefense.com: https://www.orangecyberdefense.com/dk/blog/research/for-a-safer-digital-society-breaking-down-gender-barriers-in-cybersecurity

CyberPeace Institute. (2024, March 21). *Cyber Peace Institute*. Retrieved May 2024, from

© WE - Faculty of Arts

https://cyberpeaceinstitute.org/news/advancing-responsible-state-behaviour-in-cyberspace-harms-methodology/

EIGE. (n.d.). *Gear action toolbox*. Retrieved MAY 2024, from eige.Europa.eu: https://eige.europa.eu/gender-mainstreaming/toolkits/gear/training?language_content_entity=en

FDFA. (2021, July 04). *FDFA*. Retrieved May 2024, from https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2021/04/uno-cyber-normen.html

GAFCC. (n.d.). *Integrating Gender throughout the Capacity Building Facility: A Webinar Training Series.* Global Alliance for Clean Cookstoves. Retrieved May 2024, from https://cleancooking.org/binary-data/RESOURCE/file/000/000/438-1.pdf

Hogeveen, B. (2022, Feb). *The Australian Strategic Policy Institute Limited*. Retrieved May 15, 2024, from ASPI.org: https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

LEARN.ORG. (2024). *Learn.org*. Retrieved May 21, 2024, from learn.org: https://learn.org/articles/cybersecurity_barriers_for_women.html

Lewis, J. A. (2022, Feb 23). *CSIS.org*. Retrieved May 2024, from https://www.csis.org/analysis/creating-accountability-global-cyber-norms

Miller, K., Shires, J., & Tropina, T. (2021). *Gender approaches to cybersecurity: design, defence and response.* UNIDIR. doi:https://

Offenso Hackers Academy. (2023, August 24). *Offenso Hackers Academy*. Retrieved May 20, 2024, from offensoacademy.com: https://offensoacademy.com/women-in-cybersecurity/

UN Women. (2024, January 31). *UN Women, Africa*. Retrieved May 2024, from africa.unwomen.org: https://africa.unwomen.org/en/stories/news/2024/01/capacity-building-training-on-gender-responsive-migration-data-and-statistics-governance-to-contribute-on-safe-migration

UNIDIR. (2021, March 24). *UNIDIR*. Retrieved May 2024, from unidir.org: https://unidir.org/advancing-gender-considerations-in-the-cyber-oewg/

WomenTech Network. (2024). Retrieved May 21, 2024, from womentech.net: https://www.womentech.net/en-in/how-to/what-are-hidden-barriers-women-face-in-cybersecurity-and-how-can-we-overcome-them

©WE-Faculty of Arts