Introduction

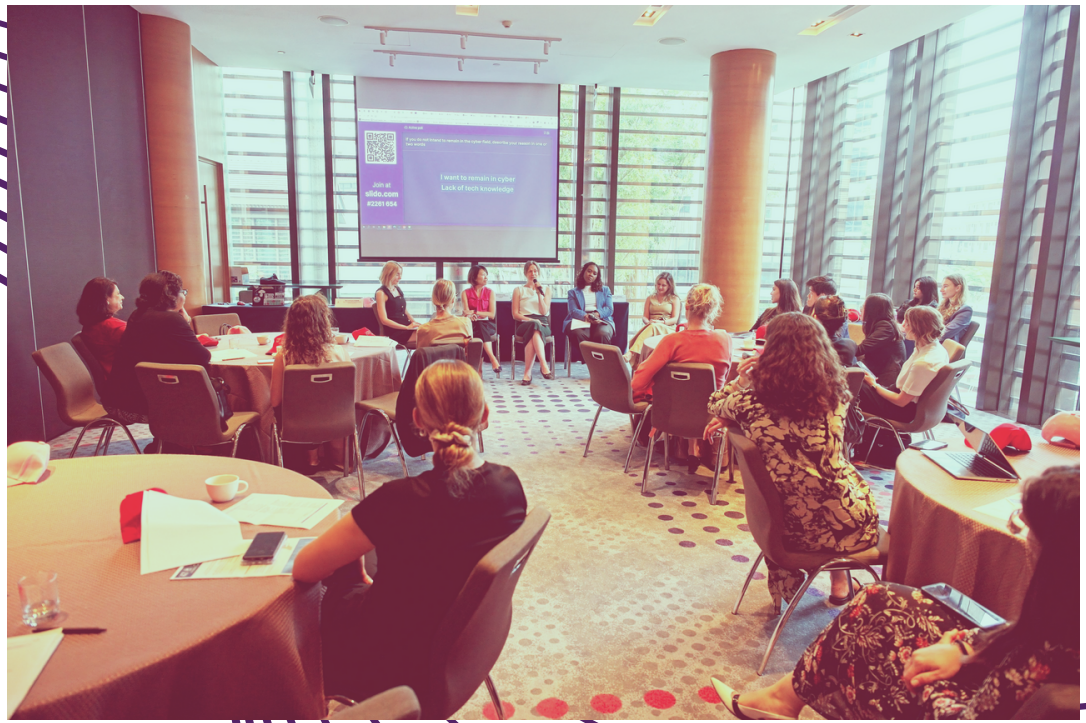
Cyber law enforcement agencies face many challenges in today's digital world. The cyber threat landscape is always changing, influenced by global criminal networks and the rise of new technologies. To address these threats, police have to work with both public and private stakeholders to bring together the best talents and the most efficient responses to national and international cyber issues.

At the same time, people's expectations are also rising. They want better services, more transparency, and a workforce that reflects the community. With these expectations, agencies are supposed to become more and more inclusive.

Based on this context, a pressing question emerges: why are women still under-represented in cyber law enforcement, and how does this impact their experiences and longevity in the field?

The report is composed of three sections: **Challenges, Opportunities, and Best Practices.** It is derived from the insights, expertise, and shared experiences of speakers and panelists of the inaugural INTERPOL Workshop on Women in Cyber - complemented by the active engagement and discussion among participants of the event.

In essence, this report encapsulates the collective wisdom, concerns, and aspirations of many at the forefront of championing the cause of women in cyber law enforcement.



PRIORITY 1: CHALLENGES

"Not enough cooks in the kitchen"

In recent times, the importance of gender diversity in the realm of cyber law enforcement has taken centre stage. Notwithstanding commendable efforts, a palpable void remains in the representation of women in this sector.

During the INTERPOL workshop on Women in Cyber, many challenges were identified and discussed. Amongst them:

Representation Deficit: The under-representation of women in cyber law enforcement not only affects the numbers but limits the potential range of strategies to combat cyber threats. Diverse teams bring in richer perspectives which are crucial in identifying and combating multifaceted cyber threats.

Technological Stagnation: Despite the rapid pace of technological advancements, there is an evident lag in the domain of cyber breach control. This gap heightens vulnerabilities, underscoring the need for diverse thinkers to bridge the disconnect between technological progress and its security applications.

Leadership Disparity: While society advocates for gender equality in leadership, a noticeable gap exists in women's representation in leadership roles within cybersecurity. This disparity robs the sector of unique perspectives that women leaders can offer.

Myth and Misconception: Cybersecurity is often misconceived as a purely technical field, sidelining potential talents who could offer different insights. Additionally, viewing gender challenges as solely women's issues detracts from the collective responsibility needed to address them.

Cultural and Regional Barriers: Regional disparities, like the notable lack of women in cyber law enforcement roles in Africa, emphasize the complexities of gender challenges in different parts of the world. Strategies should be designed considering these regional and cultural nuances.

Shared Responsibility: There is a need to move beyond viewing gender-related challenges as exclusive to women, and recognize them as an industry-wide issue demanding collective action.

FOCUS AREA 2: OPPORTUNITIES

"The only way parity will increase is if we talk about diversity as a business problem and give it the same rigor and cadence that we do for other business "

The domain of cyber law enforcement, though riddled with challenges, presents also an array of opportunities to enhance gender inclusivity. With the right strategies and perspectives, these opportunities can revolutionize the way women partake in this sector.

During the INTERPOL workshop on Women in Cyber, many opportunities were identified and discussed. Amongst them:

Behavioural Insights in Recruitment: The shift towards considering behavioural attributes in hiring brings about a refreshing change from the traditional technical-focused approach. This ensures that teams consist of individuals who are not only technically skilled but also possess crucial behavioral attributes like empathy, problem-solving, and conflict resolution. Embracing this avenue opens the door for a holistic and effective cybersecurity team.

Strategic On-The-Job Training: The growing emphasis on training as opposed to pre-existing technical knowledge offers a substantial opportunity. Tailored training programmes, especially for women, can mitigate knowledge and confidence disparities. Supported by mentorship and guidance, women can adeptly transition into and excel within cybersecurity roles. These are offered by national, regional, and international authorities and organisations, like the Women, Peace and Cybersecurity in Asia Pacific.

Gender-Integrated Toolkits: With institutions like Chatham House leading the charge, there is a rise in gender-centric frameworks designed specifically for cybersecurity. These standardized toolkits provide actionable guidelines, promoting the integration of gender-conscious perspectives in all stages of cybersecurity endeavours. Adoption of these can inherently weave gender inclusivity into the fabric of organizations.

Community Engagement and Networking: Engaging in community-driven educational platforms serves as a dual advantage. On one hand, it provides an avenue for continuous learning and upskilling. On the other, it offers a robust networking platform. Immersing in these communities allows women to connect with peers, mentors, and industry experts, fostering a supportive environment. Such interactions amplify collective growth and underscore the importance of women in cyber roles.