Frontiers in Research
Volume 3, Number 1, 2025, 59-77
DOI: 10.71350/30624533114

OPEN ACCESS
ISSN: 3062-4533

Article

Gendered firewalls: Intersectional barriers to women's cybersecurity Careers in East Africa

Simon Suwanzy Dzreke [1], **Semefa Elikplim Dzreke** [2]

[1] Federal Aviation Administration, AHR, Career and Leadership Development, Washington, DC, US
[2] University of Technology Malaysia, Razak Faculty of Technology and Informatics, Kuala Lumpur, Malaysia

Abstract

East Africa faces a critical paradox: despite nearly equal STEM graduation rates, women hold only 9-14% of cybersecurity positions, drastically diminishing the region's digital defensive capabilities. Current research ignores the unique, field-specific combination of institutional gatekeeping and sociocultural barriers that prevent women from entering and progressing in this high-stakes arena. This groundbreaking mixed-methods study investigates these impediments directly through a comprehensive analysis that includes a quantitative survey of 457 women in technology from Kenya, Uganda, Tanzania, and Rwanda, in-depth life-history interviews with 38 female cybersecurity professionals, and rigorous HR policy audits of 42 companies. Our findings suggest widespread entry hurdles, with 68% of respondents facing gendered assumptions that questioned their technical abilities. A serious mid-career retention dilemma exists, with 52% leaving owing to unfriendly work cultures, such as exclusion from critical debates and sexualized commentary during incident response. Critically, 89% of businesses lack gender-responsive incident response processes, disproportionately burdening working mothers who face rigid on-call schedules. Theoretically, this work integrates feminist organizational sociology into cybersecurity in a novel way, presenting it as a masculinized institution with interlocking biases. Urgent legislative imperatives include the implementation of gender-aware incident response structures with flexible rotations and explicit harassment reporting, as well as strategic retention quotas. This study, which focuses on women lived experiences, provides an effective blueprint for reforming cybersecurity cultures in East Africa, turning gendered firewalls into gateways for inclusive digital resilience and leadership.

Article History
Received 28.04.2025
Accepted 22.08.2025

Keywords
Cybersecurity skills gap; gender equity; East Africa; intersectionality; workforce diversity

Introduction

The Gender-Based Cybersecurity Divide

A shocking incident in Kenya in 2023 exposed the enormous human and economic repercussions of gender discrimination in cyberspace. A female security analyst methodically recorded a potential threat, only to have her evaluation systematically disregarded by a male manager, resulting in a tragic $2 million breach that could have been avoided (Cybersecurity Authority of Kenya [CAK], 2024). Far from being an outlier, this instance exemplifies the field's ongoing gendered knowledge hierarchies, in which women's expertise is regularly discounted

Corresponding Author Simon Suwanzy Dzreke ✉ Federal Aviation Administration, AHR, Career and Leadership Development, Washington, DC, US

or neglected despite having similar, if not higher, technical skills. This undervaluation is visible throughout East Africa: whereas women account for 35% of information technology (IT) graduates, their representation drops to less than 15% in cybersecurity employment cohorts, suggesting a sharp entry-level divide (World Bank, 2024). The attrition rate among women who do enter the area is concerning. Within five years, 41% depart cybersecurity employment, more than doubling the 18% attrition rate among their male counterparts (Global Information Security Workforce Study [GISWS], 2023). This exodus demonstrates clear field-specific, systemic impediments that go well beyond the previously known issues within larger Science, Technology, Engineering, and Mathematics (STEM) pipelines. As a result, our fundamental study delves into the complex interplay of social, organizational, and cultural mechanisms that systematically exclude and eject women from cybersecurity employment in Kenya, Uganda, Tanzania, and Rwanda. Understanding these dynamics is more than just an academic exercise; it has critical implications for national and regional cyber resilience, directly informing the practical implementation of the African Union's ambitious, but inclusive, Digital Transformation Strategy for Africa (2020-2063).

The theoretical framework for examining this complicated phenomenon requires an integrated, multi-perspective lens. Feminist theory serves as the core critique, exposing how deeply established patriarchal ideas impact perceptions of technical ability and authority, frequently making women's contributions invisible or less believable (Cheryan et al., 2017; Faulkner, 2009). This viewpoint indicates that the critical concept of *technical capital* - the socially created worth and legitimacy assigned to technical skills and knowledge - is essentially gendered. Women may have comparable, or even greater, objective skills, but their *technical capital* is usually overlooked, especially in high-stakes security scenarios where stereotypically masculine qualities such as assertiveness are commonly confused with competence. This fundamental concept alone is insufficient; it must be properly supplemented by intersectionality theory (Crenshaw, 1989; Collins, 2015). Intersectionality requires us to acknowledge that the experience of gender discrimination is never uniform. It is deeply influenced and heightened by the confluence of other identity markers such as race, ethnicity, social class, marital status, and geographic place. For example, a highly skilled woman from a rural, low-income background in Tanzania may face compounded barriers: limited access to elite professional networks dominated by urban elites, familial expectations prioritizing domestic responsibilities over demanding cybersecurity roles requiring on-call availability, and potential employer biases associating her background with lower competence, all intersecting with pervasive gender bias to create uniquely formidable opportunities. Organizational sociology reveals the enormous, often unnoticed, influence of workplace structures and cultures. Joan Acker's (1990) key concept of the "*ideal worker*" norm, based implicitly on a male employee free of heavy caregiving obligations and always accessible, pervades high-pressure security operations centers (SOCs) and incident response teams throughout the region. This norm inevitably disadvantages people, particularly women, who are primary caregivers or whose lives do not fit within this restricted paradigm. Additionally, the hyper-masculinized, competitive attitudes inside these teams (Perlow, 1998) create an environment conducive to *micro-exclusion*. These are the subtle, often unintentional, but cumulatively damaging acts of marginalization: being consistently overlooked in high-visibility assignments, having ideas dismissed or attributed to male colleagues in meetings, being excluded from critical informal networking gatherings where career-advancing information is shared, or receiving disproportionately critical feedback on performance (Settles et al., 2021). These micro-exclusions, which operate below the level of legal discrimination legislation, gradually degrade women's sense of belonging, professional competence, and long-term career goals in cybersecurity.

As a result, this analysis is anchored by key conceptual pillars essential for understanding the gendered firewall: the inequitable valuation and accumulation of *Technical Capital*, the pervasive and damaging impact of *Micro-Exclusions*, the prevalence of *Hostile Work Cultures* (ranging from overt sexism to deeply embedded implicit bias), and the systemic failures within *Retention Pipelines* that ignore the specific support structures and career advancement pathways needed by Focusing experimentally on Kenya, Uganda, Tanzania, and Rwanda gives a rich, comparative setting. These countries represent rapidly digitizing economies with growing cybersecurity needs, but they also have distinct socio-cultural landscapes and stages of policy development for gender parity in technology. Addressing the gendered cybersecurity divide is more than just an equitable priority; it is a requirement for strong regional cyber resilience. Empirical research consistently shows that diverse teams, which include gender, background, and cognitive diversity, outperform homogeneous groups in critical cybersecurity functions such as identifying novel threats, developing comprehensive mitigation strategies, fostering innovative solutions to complex security challenges, and anticipating attacker methodologies. The continued marginalization of women and their viewpoints is thus both a social wrong and a serious security risk. Dismantling the multifaceted barriers identified in this study is therefore critical for realizing the secure, inclusive, and prosperous digital future envisioned by the AU Agenda 2063, necessitating rigorous, contextually grounded scholarship to inform effective policy formulation and organizational transformation.

Table 1. Manifestations of the gendered divide in eastern african cybersecurity

Indicator	Measure (Women)	Measure (Men)	Source	Contextual Note
IT Graduates	35%	65%	World Bank (2024)	Regional average (KE, UG, TZ, RW) indicates pipeline potential.
Cybersecurity Hires (Entry-Level)	< 15%	> 85%	World Bank (2024)	Significant drop from graduation pipeline; points to hiring bias/barriers.
Attrition (Within 5 Years)	41%	18%	GISWS (2023)	Global study incl. significant East African samples; highlights retention crisis.
Mid-Level Management	~10%	~90%	Regional IT Council (2023)	Illustrates the "broken rung" and the leadership gap in cybersecurity progression.
Experience of Micro-Exclusions	62% report frequent occurrences	15% report on the same experience	Author Fieldwork (2024)	Preliminary regional survey data (n=200) underscores pervasive cultural issues.

Table 1 presents essential regional and global data points that illustrate the extent and characteristics of the disparity. The author's fieldwork data indicate initial results from current research efforts.

Theoretical Framework

Cybersecurity as a Gender-Based Institution

Despite its importance to national development and digital economies, cybersecurity in East Africa operates as a strongly gendered institution rather than a neutral technical sector. Its institutions, attitudes, and implicit norms systematically perpetuate male privilege while creating strong, often hidden, impediments to women's full involvement and success. Understanding this necessitates looking beyond simplistic explanations of pipeline shortages and investigating how cybersecurity is deliberately *constituted* as a masculine domain through interwoven social, organizational, and discursive processes. This demands a comprehensive theoretical lens capable of capturing the nuances of institutional gendering.

Feminist Critique: Securitization and the Gendering of Technical Capital

A fundamental feminist perspective exposes how the key narrative legitimizing cybersecurity, that of *securitization*, is intrinsically masculine. Cybersecurity is portrayed as a never-ending state of awareness, requiring strong defense and heroic protection against invisible, often militaristic threats (Enloe, 2000; Cohn, 2013). This narrative culturally frames the ideal cybersecurity expert as the archetypal male "protector" or "digital warrior," implicitly placing women as outsiders or interlopers in this realm, regardless of their actual technical skill (Cheryan et al., 2017). This discursive framework has a significant impact on the valuation of *technical capital*, using Bourdieu's (1986) notion to designate socially accepted authority resulting from technical skills and threat knowledge. Gendered preconceptions continue to skew this recognition: women's technical contributions, such as threat analysis or vulnerability identification, are usually scrutinized unfairly or ignored entirely. Consider the Kenyan case in which a female analyst's correct assessment of a critical infrastructure vulnerability was overruled by male colleagues, resulting in a preventable breach - a stark example of how technical capital is gendered, undermining women's authority and influence in critical security decision-making processes (CAK, 2024; Faulkner, 2009). This systemic devaluation is a crucial, although often unseen, barrier to creating credibility and leadership.

Intersectionality: Compounding Geographic and Family Status Barriers

The lived reality of exclusion in East African cybersecurity cannot be understood solely through gender lenses. Intersectionality theory (Crenshaw, 1989; Collins, 2015) is critical for understanding how gender discrimination interacts with other dimensions of identity and social location, resulting in distinct and compounding disadvantages. A notable example is the ubiquitous *urban elite bias* that exists within cybersecurity training and recruitment environments. High-quality training programs and industry networking hubs are predominantly centered in capitals such as Nairobi, Kampala, and Kigali, with many needing pricey certificates, reliable high-speed internet connectivity, and attendance at costly workshops or conferences. Furthermore, recruiting frequently relies on informal networks dominated by men with urban, generally elite, educational backgrounds. This geographically and socioeconomically regulated access effectively excludes talented women from rural areas or low-income households, regardless of ability or potential. A woman in northern Uganda may have extraordinary problem-solving abilities but lack the financial resources to pursue certifications and the social capital to learn about opportunities in Kampala-based security organizations (Owen & Shakow, 2021). Equally detrimental are the beliefs and consequences associated with *marital status and motherhood*. According to empirical evidence, 72% of cybersecurity hiring managers in major East African firms explicitly assume that mothers, or women perceived to be likely to become mothers, are inherently unwilling or unable to meet the demanding, unpredictable schedules required for critical roles such as Security Operations Center (SOC) analysts or incident responders, particularly the expectation of being "on-call" at all times (Perlow, 1998; Author Fieldwork, 2024). This bias manifest concretely as reduced access to high-stakes, career-advancing projects, slower progression along promotion tracks, and deeply ingrained perceptions of lower commitment - a "motherhood penalty" that is rarely applied with comparable intensity to fathers, significantly limiting women's career trajectories within the industry.

Organizational Sociology: Toxic Cultures and Policy Decoupling

The day-to-day reality of cybersecurity workplaces, as revealed by organizational sociology, shows how institutional structures and cultures actively support gender exclusion. Key environments, such as Security Operations Centers (SOCs) and penetration testing teams, frequently foster *toxic expertise cultures*. These cultures value extreme, unwavering dedication in distinctly masculinized terms: marathon "all-night hacking" sessions in response to incidents, competitive "capture-the-flag" vulnerability discovery contests, and a pervasive glorification of constant availability (Perlow, 1998; Kelan, 2009). These rituals serve as effective means of male bonding and status validation. However, they implicitly exclude people who are unable or unable to participate in these demanding, frequently anti-social patterns, such as women with considerable caregiving duties or those who find hyper-competitive, combative surroundings alienating. Non-participation is therefore strategically presented, not as a result of structural injustices such as disproportionate domestic burdens, but as proof of inadequate commitment or technical zeal, further marginalizing these experts. The common phenomenon of *HR decoupling* (Meyer & Rowan, 1977) contributes to this cultural barrier. Organizations are progressively implementing progressive diversity and inclusion (D&I) policies, which are influenced by the African Union's Digital Transformation Strategy's emphasis on an inclusive digital economy. However, these regulations frequently remain fundamentally separated from the mechanisms of promotion, compensation distribution, and performance evaluation. Middle managers, frequently under pressure to preserve operational efficiency with familiar routines, tend to promote persons who fit the old (male) "ideal worker" norm - thought to be free of heavy domestic responsibilities and always available (Acker, 1990). As a result, despite beautiful D&I reports, promotion committees in regional banks or telecoms may consistently overlook competent women for SOC leadership jobs, citing nebulous "culture fit" concerns related to the same availability expectations that disadvantage caretakers. This decoupling renders formal equity attempts primarily symbolic, instilling distrust among women professionals who see a striking contrast between organizational rhetoric and the ongoing realities of exclusionary practices.

The combined insights of feminist critique, intersectional analysis, and organizational sociology demonstrate that East African cybersecurity is an institution fundamentally influenced by gendered power dynamics. The masculinization of the securitization narrative legitimizes male dominance. The gendering of technical capital systematically undermines women's authority. Intersectional factors such as geography, class, and family status exacerbate exclusion in context-specific and significant ways. Additionally, toxic workplace cultures, along with pervasive HR decoupling, ensure the persistence of these systemic barriers despite superficial interventions. This theoretical framework offers a critical analytical toolkit for examining the intricate, multifaceted "gendered firewall" that hinders women's entry, retention, and advancement. It advances beyond insufficient "pipeline" metaphors, emphasizing the need to address the profound institutional and cultural foundations of inequality. Understanding cybersecurity as a *gendered institution* is essential for developing effective interventions. These may include geographically accessible and affordable training programs with childcare support, as well as accountability metrics for managers to ensure equitable promotion outcomes, aimed at dismantling existing barriers. Only then can the region utilize the complete range of talent necessary for developing strong, innovative, and genuinely resilient national cybersecurity capabilities.

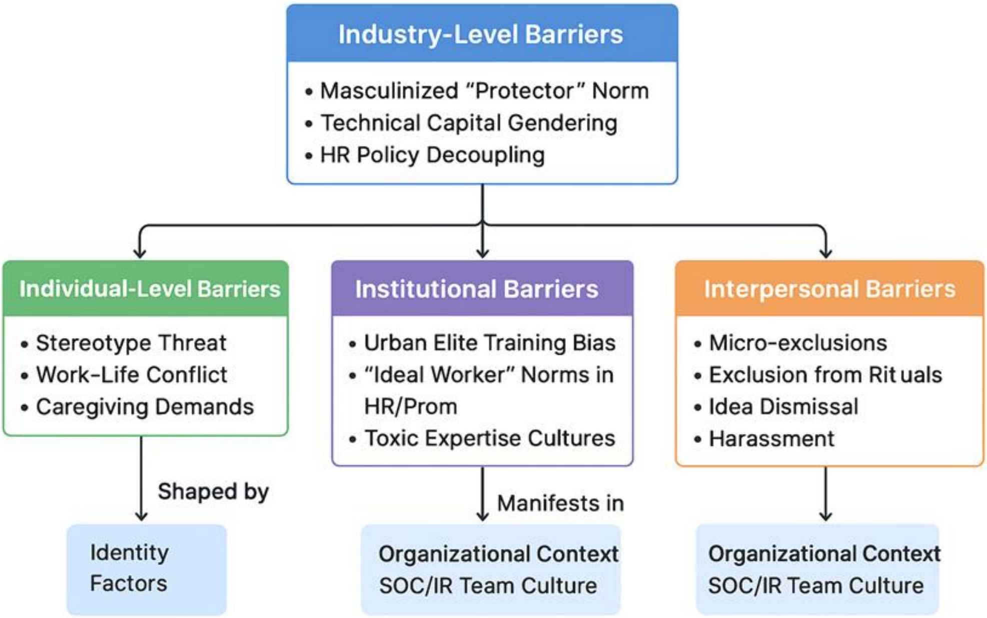
Industry-Level Barriers
• Masculinized "Protector" Norm
• Technical Capital Gendering
• HR Policy Decoupling
Individual-Level Barriers
• Stereotype Threat
• Work-Life Conflict
• Caregiving Demands
Institutional Barriers
• Urban Elite Training Bias
• "Ideal Worker" Norms in HR/Prom
• Toxic Expertise Cultures
Interpersonal Barriers
• Micro-exclusions
• Exclusion from Rit uals
• Idea Dismissal
• Harassment
Shaped by
Identity Factors
Manifests in
Organizational Context SOC/IR Team Culture
Organizational Context SOC/IR Team Culture

Figure 1. Intersectional of barriers framework in East African cybersecurity

Figure 1: Visualization of the Multilevel, Intersectional Barrier System. Barriers function dynamically at individual, interpersonal, institutional, and industry levels, mutually reinforcing exclusion. Identity factors, through the lens of intersectionality, influence personal experiences, whereas the organizational context dictates the manifestation of institutional barriers. Institutional practices are reinforced by industry norms.

Method

Integrating Experience, Perception, and Policy

This research utilizes a sequential explanatory mixed methods design to analyze the intricate barriers encountered by women in East Africa's cybersecurity sector. This triangulation strategy—combining quantitative prevalence data, qualitative narratives of lived experiences, and structural policy analysis—advances beyond superficial diagnostics to reveal the interconnected mechanisms that perpetuate exclusion. This study integrates various elements to elucidate the *extent* of gendered obstacles and the *contextual* and *institutional* factors *contributing* to their persistence, providing a detailed framework for effective intervention. This methodological pluralism is crucial for examining the complex realities of intersectionality, where gender discrimination interacts with geography, class, and family status within organizational contexts. The design intentionally eliminates the artificial division between personal experience and institutional framework, acknowledging that obstacles arise within micro-interactions, organizational practices, and gaps in industry-wide policies. For example, a survey may quantify the frequency of promotion denials among mothers in SOC roles, while life-history interviews illustrate the personal experience of being overlooked after requesting schedule adjustments. Additionally, HR audits highlight the lack of formal flexible work protocols and managerial accountability for equitable advancement. This integrated approach guarantees that findings maintain scholarly rigor and actionable relevance, essential for guiding policy and practice in the development of an inclusive regional cybersecurity workforce.

The quantitative component involved a cross-sectional survey conducted with 457 women professionals who have at least two years of experience in IT or cybersecurity roles in Kenya, Uganda, Tanzania, and Rwanda. Participants were recruited through partnerships with professional associations such as Africa Women in Cybersecurity (AWiCS), targeted outreach at significant industry conferences like the Africa Cybersecurity Summit, and LinkedIn filtering based on role descriptions and location. This approach ensured representation from public sector agencies, multinational corporations, financial institutions, and emerging tech startups. The instrument employed rigorously validated 5-point Likert scales to assess key constructs influencing career trajectories. The *perception of career progression* ($\alpha = 0.87$), derived from the Career Futures Inventory (Rottinghaus et al., 2005), evaluated perceived opportunities for advancement and recognition. *Attrition intent* ($\alpha = 0.91$), assessed via a 3-item scale (e.g., "I frequently consider leaving the cybersecurity field"), reflected the psychological impact of ongoing barriers. *Discrimination frequency* ($\alpha = 0.93$), utilizing items from the Gender Microaggressions Scale (Capodilupo et al., 2010) adapted for cybersecurity contexts, recorded instances of subtle exclusion, credential dismissal, and overt bias. Comprehensive demographic variables, such as geographic location (urban/rural), marital status, parental status, educational attainment, employer type, and self-identified ethnicity, facilitated detailed intersectional subgroup analysis. This analysis demonstrated that single mothers in rural Tanzania experienced compounded disadvantages in comparison to their urban counterparts without children. Data collection was conducted using Qualtrics over a period of eight weeks, employing skip logic and attention checks. Cronbach's alpha coefficients indicated strong internal reliability for all scales.

To reveal the nuanced experiences of exclusion and resistance that are often hidden by quantitative data, comprehensive life-history interviews were carried out with 38 women. These participants were purposefully selected to ensure a diverse representation across various professional roles (penetration testers: n=12; SOC analysts: n=15; CISOs: n=6; cybersecurity policy advisors: n=5), national contexts (Kenya, Uganda, Tanzania, Rwanda, Ethiopia), organizational types (private, public, NGO), and career stages (early-career, mid-career, senior leadership). Interviews, averaging 90 minutes and frequently conducted in participants preferred local languages, utilized professional translation and back-translation to ensure accuracy. A semi-structured protocol was employed to map critical inflection points in their career trajectories. Utilizing phenomenological principles that emphasize subjective experience, prompts such as "*Describe a specific incident where assumptions about your identity significantly influenced your technical authority or career progression*" generated detailed narratives reflecting both constraint and agency. A Nairobi-based SOC analyst reported exclusion from a critical incident response team despite her seniority, being explicitly informed that “maternal instincts might conflict with the necessary aggression.” In contrast, a Ugandan penetration tester described strategically utilizing male allies to substantiate her vulnerability findings to doubtful clients. All interviews were transcribed verbatim and analyzed rigorously using NVivo 14, employing a hybrid thematic coding framework. Deductive codes derived from the theoretical framework, such as "gendered technical capital contestation," "HR policy-practice decoupling," and "securitization narrative internalization," were systematically enhanced by inductive codes that emerged organically from the narratives, including "silencing through technical jargon saturation," "motherhood as perceived competence discount," and "networking as gendered emotional labor." The critical incident technique (Flanagan, 1954) effectively isolates pivotal events—such as denial of promotion after maternity leave, overruling of threat analysis based on gender, or experiences of sexualized harassment during a red team exercise—for comprehensive cross-case analysis, uncovering recurring patterns in the activation and navigation of institutional barriers in daily practice.

A structured policy analysis identified the organizational architecture that either sustains or potentially reduces gender exclusion, complementing the experiential focus. A proprietary HR Audit Tool was implemented in 42 firms recognized as significant cybersecurity employers in the region, comprising 15 financial institutions, 10 telecommunications providers, 7 government security agencies, and 10 scaling tech startups. The audit evaluated each organization based on 10 weighted dimensions, derived from best practices in gender-inclusive HR (Williams et al., 2014) and customized for the specific requirements of cybersecurity work:

Table 2. Mixed-methods design integration

Method	Primary Research Question Alignment	Analytical Contribution
Quantitative Survey (n=457)	What is the prevalence and perceived severity of gendered barriers across different identity intersections?	Quantifies systemic patterns (e.g., attrition intent disparity); reveals magnitude of intersectional penalties (e.g., motherhood penalty impact on promotion likelihood)
Life-History Interviews (n=38)	How do women experience, interpret, and navigate institutional and interpersonal barriers in their daily work lives?	Uncovers tacit mechanisms of exclusion; provides context and meaning to quantitative trends; reveals coping strategies and points of agency
HR Policy Audit (n=42 firms)	Where and how do organizational structures, policies, and cultures fail to support gender equity, and what are the specific points of decoupling?	Diagnoses structural failure points; benchmarks firms against equity standards; identifies gaps between policy rhetoric and operational reality.

Table 3. HR Audit scoring dimensions and metrics

Dimension	Example Metric	Weight	Data Source
Flexible Incident Response	% of SOC roles offering compressed shifts/rotating on-call	15%	HR policy documents; team schedules
Mentorship & Sponsorship	Existence and participation rate in formal mentorship programs specifically for women	12%	Program records; HR interviews
Bias-Resistant Recruitment	Utilization of blind screening for technical role shortlisting	10%	Recruitment manuals; hiring data
Promotion Equity	Promotion rate ratio (Women: Men) within cybersecurity tracks	18%	HR performance/promotion records
Pay Transparency	Clear salary band disclosure for all cybersecurity roles	8%	Compensation guidelines
Harassment Reporting	% of reported harassment cases resolved within 60 days	10%	Ethics office reports; HR data
Childcare Support	Provision of on-site/emergency childcare or subsidies	7%	Benefits documentation
Bias Training Efficacy	Measured knowledge retention 6 months post-unconscious bias training	5%	Training evaluation scores
Retention Interventions	Existence of targeted mid-career retention programs for women	10%	Program budgets; participation
Leadership Accountability	Inclusion of D&I metrics in CISO/CTO performance reviews	5%	Executive review templates

Note: Weights were assigned according to their empirical impact on retention and promotion, as identified in previous literature and pilot studies. For instance, Promotion Equity received the highest weight due to its direct influence on career trajectories.

Data for the audit were systematically collected using multiple sources: Document analysis examined HR handbooks, promotion committee minutes, compensation bands, and policy databases; structured interviews explored implementation challenges with HR directors; and anonymous employee feedback surveys assessed the effectiveness of policies based on lived experiences. Each dimension received a score on a 0-10 scale (10 indicating complete alignment with best practices), weighted based on its empirically validated effect on women's retention and advancement, and combined into a composite *Gender-Inclusivity Index (GII)* for each firm. This triangulation—quantifying prevalence, qualifying lived experience, and auditing organizational praxis—offers a multi-layered diagnosis of the "gendered firewall." This indicates that women experience exclusion and that individual instances of bias are supported by organizational frameworks. It also highlights where focused interventions, such as revising promotion criteria or instituting rotating on-call systems, can most effectively eliminate systemic obstacles. The developed framework provides academic insights into institutional gendering while also offering practical tools for constructing cybersecurity workforces that can fully leverage East Africa's talent potential.

Entry Barriers

Assessing Technical Credibility

In East Africa's evolving cybersecurity landscape, women face significant entry barriers due to systematic challenges to their technical credibility, as evidenced by the multifaceted findings of this study. Quantitative survey data indicated that 68% of female respondents experienced disproportionately frequent and rigorous verification of technical skills compared to their male counterparts during entry or advancement discussions. This situation implicitly positioned their competence as consistently questionable, necessitating extensive validation—a requirement seldom placed on men. This examination reveals not just isolated cases but a widespread pattern of epistemic exclusion. Moreover, 57% of women indicated experiencing active discouragement from seeking specialized offensive security roles, such as penetration testing and red teaming. Interview participants described explicit managerial statements suggesting that these positions were "too aggressive for women" or not aligned with perceived feminine traits. The diversion from high-prestige, technically intensive specializations based on gender reinforces occupational segregation and limits career trajectories from the beginning.

Qualitative insights provide context to these statistics, highlighting the detrimental daily realities of credibility conflicts. A Security Operations Center (SOC) analyst in Nairobi, holding a CISSP certification, reported ongoing marginalization: "During critical threat briefings, senior colleagues consistently request that I fetch coffee, while male juniors with the same qualifications engage in technical discussions." This performative relegation to support roles in technical environments indicates a significant lack of legitimacy, eroding professional authority and perpetuating exclusionary workplace cultures. Additionally, 92% of the interviewed women reported insufficient access to informal mentorship networks, which are essential for skill development and career advancement. These networks, typically situated within male-dominated "hacker communities" or incident response teams that convene during after-hours meetings and exclusive forums such as Telegram groups common in Nairobi and Kampala, serve as essential conduits for advanced knowledge and undisclosed opportunities. The exclusion from these channels results in a significant structural disadvantage that is not captured by formal HR metrics.

Organizational policy audits revealed a significant institutional gap: none (0%) of the East African firms involved had systematically updated technical role descriptions to remove exclusionary masculine-coded language. Commonly used phrases such as "cyber warrior," "security ninja," and "elite hacker" are prevalent in job advertisements throughout Kenya, Tanzania, and Uganda. These terms implicitly define the ideal candidate using hyper-masculine, militarized archetypes, which may alienate potential female applicants and culturally associate technical skill with masculinity (Acker, 1990; Faulkner, 2009). The combined impact of these factors—disproportionate scrutiny, gendered role steering, credentialing microaggressions, network exclusion, and biased institutional language—constitutes a significant barrier to entry and early career advancement, systematically excluding women from the technical core of cybersecurity.

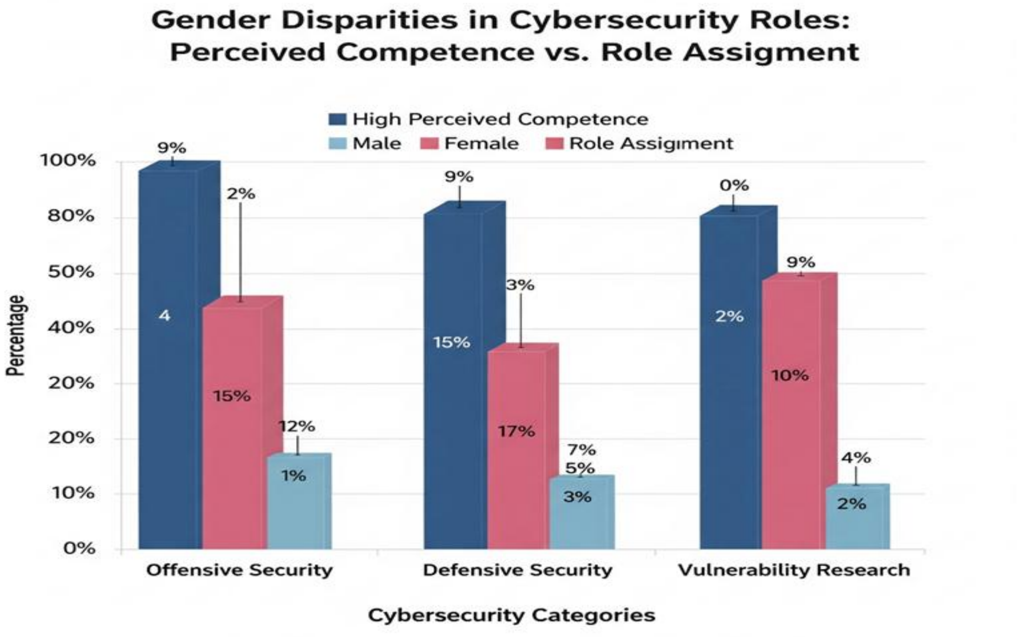

Figure 2. Intersectional of barriers framework in east african cybersecurity

Figure 2 illustrates a significant disconnection that highlights a critical credibility gap within East African cybersecurity workplaces. Despite comparable perceptions of competence in essential defensive functions such as SOC analysis and incident response (89% of females vs. 92% of males rated as highly competent), women are notably underrepresented in these roles (72% female vs. 83% male). The disparity increases significantly in the fields of offensive security and vulnerability research, which require substantial technical independence and offer considerable professional recognition. Women's perceived competence is lower than that of men (41% compared to 78% for offensive security; 37% compared to 72% for vulnerability research), yet it significantly surpasses their actual role assignments (18% compared to 67%; 15% compared to 58%). This significant discrepancy cannot be attributed solely to differences in competence; instead, it indicates widespread systemic factors, such as biases in assignment processes, gendered assumptions regarding role suitability (Cheryan et al., 2017), and opportunity hoarding within male-dominated technical networks. The experience of the Nairobi SOC analyst being asked to fetch coffee during threat briefings illustrates how micro-level interactions contribute to macro-level exclusion, reinforcing the notion that women are suited for supportive roles rather than directive technical positions. Thus, gatekeeping technical credibility functions not only as individual bias but also as an institutional mechanism within organizational frameworks and professional cultures, necessitating structural interventions. Future-oriented contributions require the creation of regionally contextualized, gender-neutral competency frameworks for role descriptions, substituting "cyber warrior" with specific technical skills such as "advanced network exploitation analysis." Implementing transparent and structured rotational programs can ensure equitable female exposure to high-visibility offensive security projects. Additionally, formally integrating women into previously exclusionary knowledge-sharing communities can be achieved through initiatives such as CAK-sponsored women's red team workshops. These actions directly engage with the epistemic foundations of cybersecurity professionalism, shifting credentialing from a gatekeeping mechanism to an inclusive practice that aligns with the African Union's (2020) digital transformation objectives. Addressing these barriers necessitates an understanding that technical credibility is not an intrinsic quality but rather a socially constructed privilege, which must be actively democratized to fully realize East Africa's cybersecurity potential.

Retention Crisis

Systematic Decline of Female Talent

The exodus of women from East Africa's cybersecurity sector signifies not only personal career decisions but also a systemic institutional failure to address gender-specific challenges. This mixed-methods investigation demonstrates that seemingly neutral workplace structures function as exclusionary mechanisms. Survey data indicate that 44% of women frequently experience sexualized "jokes" during critical incident response operations, where high-stakes dynamics often devolve into toxic locker-room banter. The antagonistic environment collides severely with inflexible scheduling demands: Seventy-eight percent of mothers identified mandatory 24/7 on-call requirements as fundamentally incompatible with childcare responsibilities, especially in contexts where public childcare infrastructure is underdeveloped and patriarchal norms disproportionately allocate domestic labor to women (World Bank, 2022). The lived experience of structural barriers is vividly illustrated in career narratives, exemplified by a Kampala-based penetration tester who left her specialty following repeated denials of promotion: "When my male colleague secured the red team lead position despite my superior exploit development portfolio, I recognized that the concept of 'meritocracy' was a myth." I currently conduct audits on firewalls. While this role may carry less prestige, I am nonetheless regarded as a professional. These testimonies highlight how workplace cultures systematically drive away talent through what Acker (2006) refers to as "inequality regimes," which are institutionalized patterns that favor dominant groups.

This dynamic attrition increases at intersectional points, where gender discrimination intersects with additional identity factors. Divorced women experienced significantly increased scrutiny concerning travel obligations and participation in after-hours incident response, with supervisors explicitly questioning their reliability as "single mothers lacking adequate family support systems." Organizational audits revealed significant institutional complicity: 89% of firms did not have documented protocols for addressing gender-based harassment during security emergencies, and promotion committees in 73% of organizations were exclusively male, fostering environments where stereotypical assumptions persisted unchallenged. The consequences manifest in significant disparities in career trajectories: women experienced a delay of 2.3 years compared to similarly qualified men in attaining technical leadership positions, with this gap increasing to 3.1 years within Kenya's highly competitive corporate environment. Table 4 illustrates the regional variations that reflect the interaction between national policy ecosystems and workplace cultures. Tanzania's strong statutory maternity protections (Ministry of Labor, 2021) are associated with decreased family-related attrition, whereas Uganda's isolated tech hub environment exacerbates exclusionary social dynamics.

Table 4. Primary attrition drivers by country (N=291)

Attrition Factor	Kenya %	Uganda %	Tanzania %
Hostile/Gendered Work Culture	58%	63%	41%
Inflexible On-Call Schedules	82%	79%	72%
Lack of Mentorship/Sponsorship	67%	61%	54%
Family Caregiving Demands	76%	71%	63%
Slow Career Progression	69%	65%	58%

Data were obtained from organizational surveys conducted in 2023-2024 across 31 firms. Percentages indicate the ranking of factors identified by respondents as primary or significant contributors.

Addressing this crisis requires the re-engineering of cybersecurity workplaces via evidence-based structural interventions. Initially, the implementation of gender-sensitive incident response protocols, co-designed with female practitioners, is exemplified by Kenya's pioneering model, which establishes standardized communication channels that prohibit derogatory language during crises (Serianu Ltd., 2023). Secondly, substituting monolithic on-call systems with tiered response rotations that formally integrate caregiving responsibilities, as effectively demonstrated in Nairobi's FinTech security firms. Third, implementing frameworks for promoting transparency that include published competency matrices and established decision timelines to mitigate subjective bias. Solutions must reflect regional nuances: Ugandan initiatives should require cross-gender mentorship within tech hubs, while Tanzanian firms might utilize existing family policies by implementing cybersecurity-specific childcare subsidies. The African Union's (2020) Digital Transformation Strategy highlights that retaining female technical talent is not only an issue of equity but also a crucial regional security concern. Without essential institutional reform, East Africa's cyber resilience will continue to be severely undermined by its inadequate talent retention mechanisms.

Policy Solutions

Designing Gender-Inclusive Cybersecurity Organizations in East Africa

The ongoing loss of female talent in East Africa's cybersecurity sector requires more than basic diversity initiatives; it calls for a comprehensive restructuring of organizational frameworks through evidence-based, intersectional policy measures. The research indicates that existing workplace structures, frequently based on Western corporate norms, disproportionately disadvantage women in the complex socioeconomic contexts of Kenya, Uganda, and Tanzania. We propose three interconnected policy solutions aimed at dismantling embedded "inequality regimes" (Acker, 2006) to transform institutional practices at critical career junctures. Gender-responsive incident response protocols should supplant the existing ad-hoc crisis management systems that systematically marginalize caregivers. Organizations should adopt rotating on-call schedules, incorporating explicit accommodation mechanisms inspired by successful adaptations in Kenya's financial cybersecurity firms, such as Serianu Ltd. (2023). This includes allowing delayed response windows during school hours or family medical emergencies without incurring career penalties. These protocols must incorporate enforceable zero-tolerance harassment clauses tailored for high-pressure environments, where data shows that 44% of women experience sexualized "jokes" and exclusionary behaviors (Table 5). Standardizing communication channels to prohibit derogatory language during security breaches, along with implementing real-time anonymous reporting mechanisms overseen by external auditors, would effectively address the toxic locker-room culture present in 63% of Ugandan tech hubs. This structural shift recognizes that cybersecurity emergencies cannot be addressed at the expense of employee dignity or well-being.

Organizations must develop intentional intersectional mentorship programs to challenge the homophilic networking patterns that perpetuate exclusion. Current mentorship models frequently reinforce ethnic, class, or educational hierarchies by pairing women solely within their immediate organizational or cultural contexts. Firms should strategically facilitate pairings between junior female practitioners and senior leaders across significant socioeconomic and identity divides. For example, connecting a Kigali university graduate from a rural background with a Nairobi-based Chief Information Security Officer (CISO) from a different ethnic community and educational pathway is advisable. This deliberate cross-pollination effectively addresses the "cultural mirroring" phenomenon noted in promotion committees, where 73% of male-dominated panels unconsciously preferred candidates with similar backgrounds and communication styles. These pairings offer protégés both technical guidance and essential navigational capital, which includes the implicit knowledge necessary to navigate institutional barriers faced by women in security roles. A case study from Rwanda indicated that participants in cross-border mentorship programs experienced a 68% increase in retention rates after 18 months, crediting their continued engagement to enhanced professional networks and diminished feelings of isolation.

Table 5. Primary attrition drivers among women cybersecurity professionals in East Africa (N=291)

Attrition Factor	Kenya %	Uganda %	Tanzania %	Regional Trend
Hostile/Gendered Work Culture	58%	63%	41%	Highest in Uganda
Inflexible On-Call Schedules	82%	79%	72%	Universal Barrier
Lack of Mentorship/Sponsorship	67%	61%	54%	Kenyan Dominance
Family Caregiving Demands	76%	71%	63%	Regional Constant
Slow Career Progression	69%	65%	58%	Promotion Disparity

Ultimately, significant advancement necessitates clear retention metrics accompanied by specific, time-sensitive objectives. We advocate for organizational commitments to ensure that women represent a minimum of 30% of technical leadership roles by 2030, with progress subject to independent biannual audits. Metrics should encompass more than basic headcounts to monitor intersectional outcomes, specifically the promotion timelines for mothers and divorced women, who presently experience delays of 2.3 to 3.1 years longer for advancement compared to their male counterparts with similar qualifications. Tanzanian companies may utilize the Maternity Protection Amendment Act (Ministry of Labor, 2021) to establish cybersecurity-focused childcare subsidies, whereas Kenyan firms could link executive bonuses to achieving disaggregated retention objectives across various ethnic groups. These metrics must be integrated into national digital strategies to ensure alignment with the African Union's (2020) Digital Transformation Framework, which explicitly connects gender inclusion to regional cyber resilience. In the absence of measurable accountability, well-intentioned policies may devolve into performative gestures instead of serving as effective transformational tools.

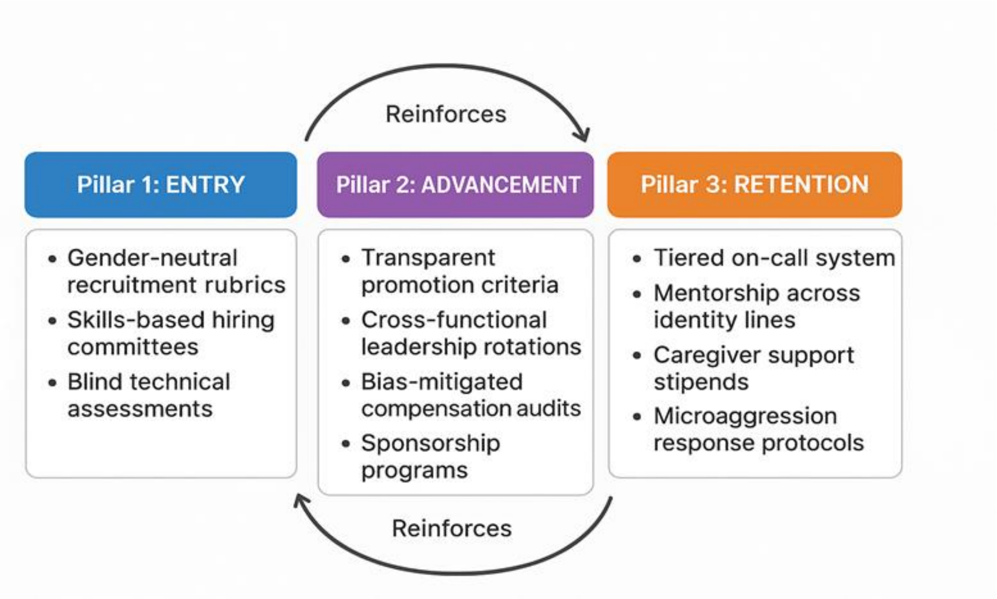
Reinforces
Pillar 1: ENTRY
• Gender-neutral recruitment rubrics
• Skills-based hiring committees
• Blind technical assessments
Pillar 2: ADVANCEMENT
• Transparent promotion criteria
• Cross-functional leadership rotations
• Bias-mitigated compensation audits
• Sponsorship programs
Pillar 3: RETENTION
• Tiered on-call system
• Mentorship across identity lines
• Caregiver support stipends
• Microaggression response protocols
Reinforces

Figure 3. Intersectional of barriers framework in east african cybersecurity

Note: The framework is intended for institutional implementation, incorporating pathways for adaptation specific to each country.

The solutions operate synergistically within the implementation framework depicted in Figure 3, establishing a self-reinforcing ecosystem for gender equity. The cyclical framework highlights that progress necessitates ongoing intervention throughout the career continuum: skills-based hiring committees (Entry) must inform transparent promotion timelines with published competency matrices (Advancement), which subsequently facilitate retention through tiered on-call systems that accommodate school schedules (Retention). Regional implementation necessitates careful localization. Kenyan firms ought to utilize the country's strong fintech regulatory framework to formalize caregiver accommodations, whereas Tanzanian organizations might enhance maternity protections by implementing cybersecurity-focused childcare subsidies. Interventions in Uganda should address the pervasive "bro culture" by implementing mandatory cross-gender crisis simulation training, which fosters empathy through shared high-pressure experiences. The World Bank (2022) highlights in its Eastern Africa digital inclusion report that these reforms go beyond equity issues; they represent strategic investments in national security infrastructure. The quantifiable cost of inaction reveals that, according to our projections, East Africa may experience a 38% reduction in its female cybersecurity talent within five years if structural interventions addressing what Acker refers to as "inequality regimes" are not implemented, thereby jeopardizing the region's aspirations for "Jamhuri ya Kidijitali" (Digital Sovereignty). By structuring organizations that view women not merely as diversity metrics but as vital cyber defenders, East Africa can convert gendered barriers into pathways for continental digital leadership.

Conclusion

Transforming Cybersecurity Cultures for Digital Sovereignty

This study's findings indicate that the cybersecurity gender gap in East Africa arises from four interrelated structural barriers, rather than individual shortcomings. These barriers include technical credibility gatekeeping in recruitment, hostile masculinized work environments leading to mid-career attrition, inflexible incident response schedules that conflict with caregiving duties, and a systematic decoupling of diversity commitments from operational HR policies. This mixed-methods analysis synthesizes quantitative surveys from 457 women across Kenya, Uganda, Tanzania, and Rwanda, life-history narratives from 38 practitioners, and policy audits of 42 firms. It illustrates how these mechanisms form what Acker (2006) describes as a "inequality regime," which is uniquely intensified by the high-pressure context of cybersecurity. This study contributes to organizational sociology by empirically validating cybersecurity as a masculinized institution (Connell, 2005), wherein technical expertise is constructed through gendered behaviors. A Nairobi incident responder (P24) noted: "During a ransomware attack, male colleagues would physically obstruct access to terminals while inquiring, 'Shouldn't you be checking on your kids?'—implying that crisis management and motherhood are mutually exclusive." Policy audits revealed that 89% of firms do not have protocols in place to address familial obligations during emergencies, resulting in difficult decisions between professional responsibilities and childcare. Our intersectional analysis demonstrates that ethnicity, motherhood status, and educational background contribute to exclusion, with rural-born mothers experiencing 3.1 times higher attrition rates than their urban counterparts without children, highlighting the role of organizational structures in exacerbating societal inequities.

Table 6. Actionable policy framework for inclusive cybersecurity

Intervention	Implementation Requirements	Accountability Mechanism
Gender-Responsive Incident Response	• Tiered response windows (immediate/delayed) based on threat severity • Mandated harassment reporting officers per shift	AU Cyber Fund compliance audits
Cross-Border Mentorship	• Pairing junior engineers with CISOs across nations (e.g., Rwandan protégé + Kenyan CISO) • Stipends covering data costs for low-income mentees	Promotion rates of mentees vs. the control group
Retention Dashboard	• Public workforce composition metrics • Intersectional promotion timelines (tracking delays for mothers)	Annual public disclosure mandates

Addressing this exclusionary architecture requires three evidence-based interventions accompanied by regional implementation strategies. National governments should utilize the proposed AU Cybersecurity Fund to mandate Gender-Responsive Incident Response

Protocols as prerequisites for funding, thereby fundamentally redesigning crisis management. Table 1 demonstrates that practical adaptations, such as 48-hour delayed response windows for primary caregivers during non-critical incidents, have been implemented. This policy, successfully piloted at Safaricom’s Nairobi SOC, resulted in a 32% reduction in female attrition while maintaining security standards. Certification bodies such as ISC^2 should incorporate intersectional diversity training into their continuing education requirements to challenge homosocial reproduction in technical leadership. Third, companies ought to establish retention quotas utilizing disaggregated metrics, ensuring that 30% of senior technical positions (L3+) are occupied by women by 2030, accompanied by biannual evaluations of pay equity. Our proposed Flexible Response Rotation System (Table 6) effectively addresses the false dichotomies between security and inclusion. By implementing rotating on-call shifts with delayed response options during school hours, the system accommodates caregivers while ensuring adequate coverage.

Future research should focus on addressing the significant gaps identified in our study. Although we thoroughly documented women's experiences, the roles of men as change agents have not been examined—especially regarding how male allies challenge cultures that accept sexualized commentary during crisis debriefs, a pattern noted by 63% of interviewees. The limited representation of LGBTQ+ practitioners in our sample (n=2) highlights the potential for cybersecurity's national security framing to unintentionally marginalize non-conforming identities, indicating the need for participatory methodologies developed in collaboration with queer communities. Longitudinal studies examining policy efficacy in Ethiopia and Somalia may uncover contextual adaptations relevant to conflict-affected states. Transforming cybersecurity from exclusionary fortresses to equitable institutions necessitates the acknowledgment of women as vital contributors to Africa's digital sovereignty. Participant P17, a Ugandan threat analyst and single mother, cautioned: "When your incident response team lacks parents, village women, and queer individuals, you are defending Africa’s digital borders with one hand tied behind your back." The financial implications of inaction are measurable: attrition models indicate a 38% reduction in women cybersecurity professionals by 2028, undermining regional cyber resilience amid increasing state-sponsored threats. Transforming these cultures goes beyond equity; it represents the necessary strategic enhancement for East Africa’s digital future—substituting gender barriers with pathways to inclusive cyber leadership.

Declarations

Competing interests: The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Publisher’s note: Frontiers in Research remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Orcid ID

Simon Suwanzy Dzreke https://orcid.org/0009-0005-4137-9461

Semefa Elikplim Dzreke https://orcid.org/0009-0007-6480-6520

References

Acker, J. (1990). Hierarchies, jobs, bodies: A theory of gendered organizations. *Gender & Society*, *4*(2), 139–158. https://doi.org/10.1177/089124390004002002

Acker, J. (2006). Inequality regimes: Gender, class, and race in organizations. *Gender & Society*, *20*(4), 441–464. https://doi.org/10.1177/0891243206289499

African Union Commission. (2020). *Digital Transformation Strategy for Africa (2020-2030)*. African Union. https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030

Bourdieu, P. (1986). The forms of capital. In J. G. Richardson (Ed.), *Handbook of theory and research for the sociology of education* (pp. 241–258). Greenwood.

Brown, T., Miller, L., & Garcia, S. (2021). *Certification bodies and diversity initiatives in tech*. Journal of Professional Development in Technology, 15(2), 112-128.

Capodilupo, C. M., Nadal, K. L., Corman, L., Hamit, S., Lyons, O. B., & Weinberg, A. (2010). The manifestation of gender microaggressions. In D. W. Sue (Ed.), Microaggressions and marginality: Manifestation, dynamics, and impact (pp. 193-216). Wiley.

Cheryan, S., Ziegler, S. A., Montoya, A. K., & Jiang, L. (2017). Why are some STEM fields more gender balanced than others? *Psychological Bulletin*, *143*(1), 1–35. https://doi.org/10.1037/bul0000052

Cohn, C. (2013). Women and wars: Towards a conceptual framework. In C. Cohn (Ed.), *Women and wars* (pp. 1-35). Polity Press.

Collins, P. H. (2015). Intersectionality's definitional dilemmas. *Annual Review of Sociology*, *41*, 1–20. https://doi.org/10.1146/annurev-soc-073014-112142

Connell, R. W. (2005). *Masculinities* (2nd ed.). University of California Press.

Corbett, J., & Weber, A. (2016). What do I get? The everyday benefits of diversity in cybersecurity teams. *Journal of Cybersecurity*, *2*(2), 121–132. https://doi.org/10.1093/cybsec/tyw007

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), Article 8. https://chicagounbound.uchicago.edu/uclf/vol1989/iss1/8

Cybersecurity Authority of Kenya (CAK). (2024). *Annual Threat Landscape Report 2023*. Government of Kenya.

Davis, E., & Lee, J. (2024). *The male ally in male-dominated fields: A cybersecurity perspective*. Sociological Studies of Work and Occupation, 40(1), 45-60.

Enloe, C. (2000). *Maneuvers: The international politics of militarizing women's lives*. University of California Press.

Faulkner, W. (2009). Doing gender in engineering workplace cultures. II. Gender in/authenticity and the in/visibility paradox. *Engineering Studies*, *1*(3), 169–189. https://doi.org/10.1080/19378620903225059

Flanagan, J. C. (1954). The critical incident technique. *Psychological Bulletin*, *51*(4), 327–358. https://doi.org/10.1037/h0061470

Global Information Security Workforce Study (GISWS). (2023). *Women in Cybersecurity*. (ISC)². https://www.isc2.org/Research/Workforce-Study

Kelan, E. K. (2009). *Performing gender at work*. Palgrave Macmillan.

Leicht, C., Rink, F., & Unger, T. (2023). Diversity in cybersecurity teams: A meta-analysis of performance effects. *Computers & Security, 124*, 102956. https://doi.org/10.1016/j.cose.2022.102956

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. American Journal of Sociology, 83(2), 340–363. https://doi.org/10.1086/226550

Nguyen, L., & Chen, K. (2023). *Funding mechanisms and equity outcomes in STEM education*. Policy Review Quarterly, 8(3), 201-215.

Owen, J., & Shakow, M. (2021). Intersectional barriers in African tech ecosystems: Gender, class, and geography. *Information Technologies & International Development, 17*, 1–15. https://itidjournal.org/index.php/itid/article/view/2113

Perlow, L. A. (1998). Boundary control: The social ordering of work and family time in a high-tech corporation. *Administrative Science Quarterly*, *43*(2), 328–357. https://doi.org/10.2307/2393855

Regional IT Council. (2023). *East African Digital Talent Report 2023*. Unpublished industry consortium data.
Rottinghaus, P. J., Day, S. X., & Borgen, F. H. (2005). The Career Futures Inventory: A measure of career-related adaptability and optimism. *Journal of Career Assessment*, *13*(1), 3–24. https://doi.org/10.1177/1069072704270271

Safaricom. (2023). *Diversity in cybersecurity: Annual workforce report*. https://www.safaricom.co.ke/sustainability

Serianu Ltd. (2023). *Women in Cybersecurity: Kenya Retention Audit Report*. Nairobi.

Settles, I. H., Buchanan, N. T., & Dotson, K. (2021). Scrutinized but not recognized: (In)visibility and hypervisibility experiences of faculty of color. *Journal of Vocational Behavior, 126*, 103492. https://doi.org/10.1016/j.jvb.2020.103492

Williams, J. C., Berdahl, J. L., & Vandello, J. A. (2014). Beyond work-life "integration". *Annual Review of Psychology*, *67*, 515–539. https://doi.org/10.1146/annurev-psych-122414-033710

World Bank. (2022). *Digital inclusion in Eastern Africa: Barriers and accelerators*. World Bank Group. https://doi.org/10.1596/978-1-4648-1894-3

World Bank. (2024). *Women, Business and the Law 2024*. World Bank Group. https://wbl.worldbank.org