Operationalizing Welcoming in Cybersecurity Communities: How Organizers Try to Shape Culture

Carson Powers*, Aman Shah†, Jaron Mink‡, Daniel Votipka*, and Ari Schlesinger◇
*Tufts University, †New York University, ‡Arizona State University, ◇Independent Researcher

***Abstract*—Despite efforts to grow and expand the cybersecurity workforce, demand continues to outstrip supply, retention is an ongoing challenge, and the workforce lacks diversity. Prior work has found the community's culture is broadly unwelcoming with most cybersecurity professionals feeling psychologically unsafe and members of underrepresented groups, especially women, regularly experiencing harassment and hate. Many organizations have attempted to address these issues through initiatives to increase diversity, often focusing on shaping individual behaviors. Unfortunately, these efforts do not appear to have been successful broadly and have drawn backlash. For diversity efforts to take hold, prior literature has shown it is essential people feel they *belong* and are *welcome*.**

In this work, we take a systemic view of the problem, focusing on how community organizers shape systems of organizational governance to establish belonging by building a welcoming community. We interview 18 organizers from 17 cybersecurity organizations (e.g., conferences, professional associations, hacking clubs) asking how they define welcoming and try to build a welcoming culture. To build welcoming communities, organizers primarily focused on newcomers, and believed being welcoming was necessary to counteract stereotypes and toxic cultural legacies. Organizers' practices focused on shaping individual behaviors, supporting relationship building, or shaping the community's environment. Critically, most organizers relied on informal practices to set norms, rather than formal policies. Because change was often handled *individually* by organizers, they faced challenges from other individuals, discontinuity in institutional knowledge, and broader structural and social obstacles. Based on these results, we provide recommendations for more systemic approaches organizers and organizations can use to build welcoming communities.

1. Introduction

Cybersecurity, and hacker culture more generally, is not known for being welcoming. Across the community, many people experience a culture that is *unwelcoming*. Katcher et al.'s survey of 342 cybersecurity professionals found that these professionals reported low psychological safety relative to other stressful professions, such as healthcare providers and business executives [1], [2]. Psychological safety means people feel safe to express themselves and their true thoughts freely, without fear of reprisal or negative consequences [3], [4]. Psychological safety's absence indicates an unhealthy cultural context, leading to burnout [5]. Moreover, women were more likely to report severe harassment [1]. Likewise, Fulton et al.'s research in vulnerability discovery describes marginalized workers' experiences of othering, hate, and harassment [6]. These are all symptoms of cultural problems. Everyone is negatively impacted by this unwelcoming culture, but people from historically marginalized communities face more severe consequences.

To demonstrate this issue more concretely, consider the example of DEF CON. Inaugurated in 1993, DEF CON is one of the oldest and largest cybersecurity conferences in the world [7]. Attendees regularly present groundbreaking attacks [8], [9], [10], [11] and it hosts one of, if not the most, prestigious capture the flag (CTF) competitions [12]. While DEF CON is not a stand-in for all facets of the cybersecurity community or its culture, it paints a complicated picture of the cultural legacy and contemporary struggles we face. DEF CON has a reputation for having "the world's most hostile network" [13], a reputation bolstered by a "good-natured" tradition of public shaming via the Wall of Sheep for attendees using the conference network without encryption [14]; at least one White House staffer has confirmed receiving a security briefing before attending [15]; and vendors may not accept credit cards because they distrust participants [15]. However, DEF CON has taken steps to change its culture and become more welcoming. It introduced a code of conduct in 2015 [16], which states "insulting or harassing other participants is unacceptable. We want DEF CON to be a safe and productive environment for everyone" [17]. Likewise, DEF CON began publishing transparency reports summarizing known code of conduct violations [16]. DEF CON enforces its code of conduct, even going so far as issuing lifetime bans to attendees [16]. One such instance in 2022 resulted in messy public proceedings after a "prominent figure" was banned for life [18]. A defamation lawsuit filed by the banned individual (that was ultimately dismissed by the judge [19]) revealed a long pattern of abusive behavior, including sexual, verbal, and physical harassment [20]. Even with a code of conduct that has enforcement mechanisms and consequences for violations, this example illustrates that toxic behavior was tolerated for years before being addressed. *Being known for hostility and a lack of trust makes it exceedingly difficult to cultivate a welcoming community* where people feel safe, even if the code of conduct states a policy where safety is

important and harassment is unacceptable.

This culture is negatively impacting the cybersecurity industry. While many steps have been taken to grow the workforce [21], [22], [23], [24], [25], [26], [27], demand has outstripped workforce capacity for years [28], [29], [30], [31], [32]. Yet, even with more cybersecurity job openings than professionals to fill them, these jobs have a high turnover rate. In a 2025 survey, 50% of organizations reported they struggle to retain qualified cybersecurity professionals [33]. Retention problems are costly, financially and more broadly [34]. In cybersecurity work specifically, worker turnover gets in the way of building institutional knowledge to protect against complex threats. Moreover, efforts to expand the cybersecurity workforce present an opportunity to improve demographic diversity; however the workforce remains dominated by white, Asian-American, and Asian men. In a recent global survey of over 2000 cybersecurity professionals, women made up only 5% of respondents [35]. While the prior industry survey does not report race and ethnicity, other recent industry surveys show fewer than 10% of respondents identified as Latino/a/x or Black [36], [37]. These cultural issues have persisted despite several efforts attempting to make the educational pipeline and workplaces more inclusive (see Section 2.2 and 2.3), indicating a deeper problem impeding efforts to expand the workforce and retain existing talent.

Thus, in this research we turn to the broader community spaces in cybersecurity to understand efforts to address cultural issues in cybersecurity by investigating *welcoming* in the cybersecurity community. Specifically, we investigate how community organizers aim to cultivate a welcoming culture. The cybersecurity community is distributed and heterogeneous; it is comprised of several subcommunities around conferences, professional organizations, CTFs, and hacking teams [6], [38]. While [6] showed community support can counteract hostile experiences in cybersecurity, we are unaware of any investigations from the community organizers' perspective. To understand how leaders and organizers aim to influence how culture is shaped, we focused on understanding how organizers of these communities try to cultivate welcoming via the following research questions:

RQ1 How do cybersecurity community organizers define welcoming?

RQ2 What practices do cybersecurity community organizers use to develop welcoming communities?

RQ3 What challenges do cybersecurity community organizers face when trying to establish a welcoming culture?

We further subdivide RQ3. First, we investigate the forces beyond the organizers' communities (e.g., broader cultural stereotypes) that motivate cultivating welcoming (**RQ3.1**). Second, we investigate challenges organizers face when implementing welcoming practices (**RQ3.2**).

To answer these questions, we conducted semi-structured interviews with 18 organizers from 17 organizations. We asked participants to define what it means for an organization's culture to be welcoming and the steps they take to establish a welcoming culture.

We found organizers often explicitly focused on newcomers when defining a welcoming culture, though they described practices that benefit the broader (existing) community. Many participants discussed building welcoming culture as a way to counteract the often unwelcoming defaults and stereotypes of the broader cybersecurity community, such as bro culture and "genius jerks." Participants reported using several practices to develop welcoming culture, which include 1) shaping member behaviors, 2) supporting relationship development, and 3) setting the environment. Within each approach, participants primarily relied on informal practices to establish norms through soft-power levers rather than more formal rule-setting.

Our results contribute insights for other researchers and organizers regarding extant practices and challenges in shaping cybersecurity culture, particularly regarding how individual organizers strive to build more welcoming communities. We draw on organizational studies and feminist literature to identify opportunities to expand on existing welcoming practices to mitigate longstanding issues of recruitment, retention, and diversity in cybersecurity.

2. Background and Related Work

In order to understand why workforce shortages in cybersecurity remain so persistent despite calls to grow the labor force, it is essential to understand the historic and cultural context surrounding current challenges around recruitment, retention, and diversity in cybersecurity. Our approach has been informed by other areas in computing that have investigated how cultural origins continue to constrain diversity and work in their area (like [39]).

In this section, we discuss cybersecurity's cultural history to provide context. Then, we describe how prior approaches to improve participation in cybersecurity and computing broadly have frequently focused on broadening participation of marginalized communities in educational contexts. We follow this with an overview of the current state of these efforts, particularly in the face of the recent backlash to DEI. Through this discussion, we will motivate our change in focus from education and the workplace to community organizers' welcoming practices. We conclude by discussing the cultural legacy of computing, highlighting how cultural and demographics have changed over time—a legacy which continues to shape who enters the field, who stays, and who leaves—to show the community's culture is malleable and persuade the reader that with enough effort by the community growing a welcoming culture is possible.

2.1. Cybersecurity's Cultural Origins

Now we turn to cybersecurity's cultural history, starting with the hacker identity, to understand the origin and depth of our challenges related to welcoming and exclusion. The hacker identity, growing out of MIT in the 1960s, [40], is characterized by an all-consuming focus on computers and programming (to the point of working all and/or odd hours), an affinity for things (over people), and an enjoyment

of puzzles (including viewing breaking into locked/secured spaces as a game) [41], [42]—characteristics that are often stereotyped as being exclusively masculine (and thus unwelcoming to people not fitting these norms) [43]. Despite the hacker identity's masculine norms, hacker culture reveres meritocracy as a part of its foundational ethos: "hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position" [44, p. 29]. However, rhetoric does not always align with lived experiences. While a meritocracy suggests everyone is welcome, in practice, values purporting to be meritocratic often do not evaluate all people equally by their ability (and fail to account for broader social inequalities [45], [46]); rather, "meritocratic" systems frequently hold people from marginalized communities to a different, higher standard than white men [47]. Moreover, hacker social networks are often critical to success [48], [49]; these "old boys" networks privilege connections between white, well-educated men further concentrating resources within these homogeneous groups [50], [51], [52]. Moreover, *the popularization of the hacker identity in broader culture in the 1980s coincides with declining participation of women in computing* [53]. The hostile and unwelcoming cultural beliefs established during the origins of the hacker identity remain pervasive [54], [55].

Growing from hacker roots, cybersecurity has transformed from the niche hacker subculture into an essential tech industry subfield. In this landscape, adversarial thinking has become an essential way to frame the ethos of cybersecurity [56], [57]. By definition, adversariality is "characterized by conflict or opposition" and hostility [58]—characteristics that definitionally clash with welcoming and belonging. In cybersecurity training, adversarial thinking's core tenants include "understanding the attacker," defensive thinking, and strategic planning around threats, attackers, and organizational goals) [56]. In classrooms, cultivating an adversarial mindset has been framed by teaching students to steal [59] to cheat [60], and to attack and defend [61], [62]. All these facets of adversarial thinking establish cultural norms around hostility that impact perceptions of cybersecurity workers and the cybersecurity community at large. When we combine a baseline environment that centers adversariality/hostility with the pervasive and exclusionary traits associated with the hacker identity, a clear picture comes into view wherein any efforts to create a welcoming and inclusive culture in cybersecurity must contend with the cultural legacy shaping the field today.

2.2. Improving Recruitment & Retention

To address computing workforce shortages, which are particularly acute in cybersecurity [32], governmental and professional organizations have strategized ways to increase the participation of people from historically marginalized communities. In this context, historically marginalized communities can be framed as an untapped/underrepresented population that could help resolve workforce shortages and an opportunity to improve diversity, equity, and inclusion (DEI) in the tech industry. Large scale, organized efforts to "broaden participation" have been ongoing since the 1990s [63], [64], [65], [66], [67], [68]; often focused on increasing both the overall number and the ratio of women in computing [64], [69], [70], [71]. While women are often the main or initial focus of broadening participation efforts, many identity attributes (e.g., gender, race, sexuality, class, ability, etc.) and their intersections need to be addressed to change low participation and exclusion [72], [73], [74].Efforts to broaden participation typically focus on the *recruitment* of students in educational environments, often in K-12 contexts [74], [75], [76], [77], [78], [79], [80].

However, recruitment (particularly of novices in educational contexts) only addresses part of the problem; there are issues with retention of novices and experts poses substantial challenges in computing. For instance, women leave computing at faster rates than in other professions [73], [81], [82], [83], [84]. When a STEM field valorizes workaholism over work-life balance (an ethos similar to the hacker identity's all-consuming focus on programming), evidence shows this produces a "burn and churn" culture that pushes people of all identities out of the STEM workforce [47], [85]. While the focus of many prior approaches to improve workforce participation have focused on broadening participation, particularly through recruiting novices from marginalized communities in educational contexts, further work is needed to make the culture—which impacts all community members, those new and established—more welcoming.

2.3. The Current Situation: Hampered Success, DEI Backlash, & Organizational Change

Despite decades of substantive and ongoing efforts to improve participation from marginalized communities in computing, these initiatives have struggled to substantially increase participation, evidenced by a decreasing proportion of undergraduate computing degrees awarded to Black people in the U.S. [86] and less than 25% of undergraduate computing degrees awarded to women [86], [87], [88], [89]. Outcomes in cybersecurity are not largely different. This is not to say all the efforts thus far have been unsuccessful—the situation may well have been worse without these efforts; however, we are not seeing widespread success broadening participation in educational contexts across the board.

The situation in industry is not much better. Decades of corporate diversity programs have not improved recruitment and retention in the tech industry [84], [90], [91]. Worse, many of the popular initiatives considered cornerstones of DEI do not actually improve diversity *and* can ignite negative responses from the existing workforce [92], [93]. For example, corporate training about bias and harassment can exacerbate bias and harassment and make employees more defensive [92], [94]. Many existing DEI programs have been implemented without evidence of efficacy [92], [93], [95], [96]. Many more have focused on virtue signaling and/or performative compliance rather than making substantive changes for workplace diversity [93], [97]. Likewise, formal rules in bureaucracies (such as job tests, mandatory reporting, and mandatory arbitration) often fail to support, protect,

or promote people from marginalized groups; moreover, these rules do little to impact the informal power structures of these organizations and can even codify practices that further marginalize the very people diversity initiatives aim to support [92], [95], [98]. This is not to say there are no effective, evidence-based strategies for improving diversity in the workplace (see [92], [93] for effective examples); rather, it's that these effective strategies have not been the norm in the era of DEI or broadening participation in computing, especially in the tech industry.

Unfortunately, these issues are not unique to the U.S. Women frequently face discrimination in the computing workplace that leads to retention issues in many countries (even countries like India where computing education participation is more equitable) [99], [100]. Likewise, racial harassment and discrimination follows tech workers across national borders [101], [102]. *This background illustrates how hostility and discrimination are part of an unwelcoming culture that contributes to the hampered success of recruitment and retention initiatives, particularly those focused on broadening participation.*

When changing the cultural status quo like through diversity promoting efforts, resistance should be expected. Prior work confirms resistance from current employees (often white men) to changing workplace diversity is common [92], [95], [98]. Employees can feel threatened by changes to workplace diversity for several reasons, and respond by lashing out, often via sexual and racial harassment [98]. Given resistance commonly follows pushes for diversity, it is unsurprising to see the cultural evolution in computing include the emergence of the tech-bro (sometimes called *brogrammers*), an identity associated with tech industry cultural norms of sexual and racial harassment [103], [104]. Nor is it surprising to see the widespread (though not total) social and political backlash to DEI [93], [105].

The DEI backlash in the 2020s has shifted the organizational, political, and cultural landscape. Although the backlash started well before the Trump White House issued Executive Order 14151 ending DEI initiatives within and funded by the U.S. federal government [106], the fallout from this executive order was swift. Federal programs around broadening participation have been canceled, and nearly 200 terms (including generic identity descriptors like "women") can bring scrutiny to or lead to the cancellation of research grants administered by federal agencies like the NSF [107], [108], [109]. Critically, the DEI backlash has had a chilling effect; many organizations have publicly renounced, discontinued, and/or distanced themselves from DEI (both conceptually and programmatically) [93].

Even in a post-DEI world, the underlying issues of discrimination, exploitation, and inequality are important for everyone. Everyone suffers in exploitative, toxic, and hostile cultures; the majority of the population benefits from removing exploitation and oppression, and improving justice [110], [111], [112]. For example, in the context of the workplace, policies that increase workplace diversity also benefit the majority of workers (e.g., paid leave, flexible work arrangements, and childcare) [92], [93], [113]. People in marginalized communities (across intersections of gender, race, class, sexual orientation, (dis)ability, religion, etc.) often face more severe consequences in discriminatory systems, but improved conditions have widespread benefits.

In cybersecurity specifically, efforts to broaden participation are more focused on recruitment and retention of novices in educational contexts [75], [76], [77] than on broader cultural or professional context issues.

Reducing inequity, improving participation of individuals from marginalized communities, and creating more welcoming culture in cybersecurity is complicated, but culture change is attainable—especially at the organizational level. In cybersecurity, recent research has shown experiences of marginalization and toxic culture persist [1], [114], [115]. While there is no one-size-fits-all solution, a more systemic approach that moves beyond changes to individual people or programs is necessary [93], [95], [116], [117], [118]. For this reason, we chose a different scope than what has been the focus of prior literature, i.e., the community spaces where cybersecurity professionals seek support and networks outside their work and places of education.

2.4. The Shifting Labor Demographics and Culture in Early Computing Work

Taking a step back, we turn to the legacy of culture change in computing—a legacy that set the groundwork for cybersecurity's hacker identity [44], [119]—as it provides critical historic context for understanding how the culture and demographic makeup of computing and cybersecurity are sociocultural artifacts rather than unmovable, inevitable, or biologically determined outcomes. While it has become relatively common knowledge that many early computer programmers were women (e.g., Ada Lovelace, the ENIAC programmers, and Grace Hopper) [120], less well known is *the transition* of the computing profession, particularly programming, from women's work [121] (labor associated with low-skill, low-pay, and little power [122]) to men's work (labor associated with high-skill, high-pay, and high-power)—particularly white, Asian American, and Asian men [91]. In modern retellings, historic women figures in computing may seem like outliers and exceptions, which obscures how both the culture and labor demographics of the field have undergone major changes in the past.

Despite contemporary stereotypes, many careers in computing were initially considered feminized, secretarial labor. Early computers (workers who completed mathematical calculations) typically came from marginalized communities (women of all colors, people of color, etc.), often pursuing these jobs because they were prevented from getting other STEM jobs at the time [121]. With the advent of electronic computers (i.e., ENIAC) in the 1940s, human computers were recruited as programmers because programming was considered menial, rote, and routine work [123], [124]. There was a clear division of labor: *planners* (masculinized, scientific/mathematical labor) devised what needed to be implemented, and *programmers* (feminized labor) figured

out how to implement the planners' work on a physical computer [123], [124]. Computing historian Nathan Ensmenger describes how programming as a profession was "unusually welcome [to women] well into the late 1960s," with women making up at least 30% of working computer programmers [123, p. 237]. Many women enjoyed working in computing during this early, open era [53]. In the early days, the idea that programming would ever be associated with prestige and masculinity was unthinkable [124].

When it became clear programming was more than rote work—that it involved intellectual labor—the initial intended division of labor between intellectual masculinized work vs. rote feminized work broke down. In reality, to make programs work on early electronic computers required craft, ingenuity, and mathematical knowledge. Programming began to cultivate "a reputation for being incomprehensible to all but a small set of extremely talented insiders" [125, p. 125]. Over time, this reputation and the men it attracted to programming work contributed to a strong desire from early male programmers to formalize computing as an academic discipline and a "respectable" profession—a desire to professionalize and ultimately masculinize programming [43], [124], [125], [126], [127], [128]. Through the process of professionalizing and masculinizing computing (beginning in the 1950s), a variety of characteristics took shape that are now deeply ingrained cultural beliefs about computing and the people who choose to work in it: a disinterest in people (and a lack of social skills), anti-authoritarianism, individualism, innate genius, eccentricity, etc. [43], [123].

The programming profession's openness to women and its associations with feminized labor did not last. However, this history shows computing was not always associated with masculinity and other stereotypes common today; *the culture of computing is malleable, not static.* Although these historic demographic and cultural changes resulted in decreasing participation of historically marginalized groups and increasing hostile and exclusionary stereotypes in computing, they also show that while culture change is difficult, culture can and does change. Thus studying culture creation and efforts to shape modern culture in cybersecurity, particularly culture change focused on counteracting current and historic norms around hostility and exclusion, are important for contextualizing and addressing longstanding challenges related to topics like recruitment and retention in cybersecurity.

3. Methods

We conducted semi-structured interviews with organizers from a variety of cybersecurity communities to learn how they define welcoming and create welcoming spaces.

3.1. Welcoming, Organizations, and Organizers

To situate our findings, we define the scope of our focus and the types of organizations and individuals we recruited.

Welcoming. Throughout all communication with participants during the study, we chose to focus on asking participants how they developed a *welcoming community*, rather than using more academic terms like *belonging* or *DEI*. Due to the recent DEI initiative backlash (see Section 2.3), not only did we expect organizers might choose not to participate because they were concerned about engaging on a politicized topic, but more importantly, we believed the term's political nature would overshadow participants' deeper beliefs about the importance of creating an accepting community for all. As such, we instead used the broader term "welcoming" to capture our intended subject of interest. Welcoming is a term often associated with DEI, and the underlying concept is instrumental for creating cultures where diversity thrives [117], [129], [130], [130]. We define welcoming as a core feature of a community culture that signals members are wanted, will be included, and belong in said community.

Cybersecurity Organizations and Organizers. Given cybersecurity's breadth, we recruited organizers across communities cybersecurity professionals reported relying on in prior work [6], [38]. This includes academic and professional conferences, student clubs, CTFs, and professional meetups. Our interviews reveal these communities use similar practices and face common challenges in community management, despite differences, e.g., motivation and size.

As our study focused on understanding the systemic forces shaping the community, we focused on organizers rather than members. Prior work has primarily focused on individual members' experiences [6], finding individual experiences of being (un)welcomed rather than the organizing practices influencing these experiences. We consider cybersecurity community organizers as anyone who holds or has held within two years a position in a cybersecurity organization that was responsible (either via a specific position or indirectly via a principal position) for establishing their community's culture. This included senior executives, such as President or Chair, as well as community development positions for safe spaces and accessibility.

3.2. Recruitment

To recruit, we first compiled a list of professional and academic cybersecurity organizations. One researcher expanded this list via a Google search for each organization type (e.g., "cybersecurity university student club"). We then manually searched each organization's website and related online sources to find organizers' contact information or general contact options, yielding a list of 57 organizers. We emailed each organizer to request participation in a study on creating welcoming environments in cybersecurity. 27 responded and were directed to a screening survey to provide consent, their professional background, and their demographic information before scheduling an online 30-minute interview. However, three respondents chose not to participate out of concerns that participation might create issues for their organization due to circumstances like ongoing DEI backlash. Six participants did not respond when we emailed them to set up an interview time. The remaining 18 responded to a request for interview, and none withdrew

after beginning. One researcher conducted all interviews. To ensure consistency, they followed a written guide (see supplemental materials [131]). Participants were not paid for study participation. After each interview, we expanded our participant list by asking participants if they could suggest additional relevant organizations (i.e., snowball sampling). Aligning ourselves with best practices of credible post-positivist qualitative research [132, pg.49-51, pg.270-277], we ensure our findings are: (1) *rigorous* by sampling participants broadly, across communities, and continuing until we reaching conceptual saturation [133], and (2) *credible* by ensuring our recruitment and data covered prior work's reporting of relevant organizations [38], and issues within the community [19]. We stopped recruiting after reaching conceptual saturation at 18 interviews.

3.3. Interview Procedure

We began each interview with a consent form overview and reminded participants they may skip any question or withdraw at any time. The interview guide is in supplemental materials [131]. Our interviews consisted of five parts:

1) *Organization and organizer background:* We asked participants to provide background on their organization (e.g., focus, attendees' backgrounds and positions, general structure), as well as their role and responsibilities.
2) *Community Vibe:* We asked how they would describe the community's culture or "vibe", such as whether the organization was professional/hobbyist, and how this was established and/or changed over time.
3) *Welcoming and welcoming practices:* We asked participants to define welcoming and describe their practices to ensure their community was welcoming. We had them recall specific community experiences that made them feel (un)welcome. We did not define welcoming to participants to avoid biasing organizers' responses.
4) *Conflicts, resolutions, and code of conducts:* Participants were asked to describe an example conflict within their organization, how they deal with conflicts, and whether they have an established code of conduct.
5) *Perspectives on DEI:* Lastly, we asked participants about their opinion on DEI in contrast to welcoming in a community like theirs and whether recent events have affected either of these.

Pilots. We conducted two pilot interviews to ensure question clarity and research question coverage. After the first pilot, we changed the terminology to less formal language, asking about the community's "vibe" rather than "values" or "social norms." We did not change the protocol after the second pilot and included this participant's responses in our dataset.

3.4. Analysis

Interviews were recorded and transcribed with Zoom's built-in transcription service. Two researchers reviewed each transcript while consulting the audio to fix transcription errors. Once verified, two researchers used iterative, inductive open coding to analyze all transcripts [134]. Both researchers coded interviews independently, meeting after each to resolve disagreements and refine the codebook to capture previously unseen ideas and improve clarity. Interview segments were shared with the full research team after every interview to provide additional feedback. Because this work is exploratory, the goal of our analysis was to identify broader themes and concepts rather than agreement, as "codes were the process and not the product" [135]. As such, we followed best practices and did not calculate inter-rater reliability. After all interviews were coded, we performed axial coding to identify higher-level themes and relationships within and between codes [134, pg.123-142]. Developing the codebook was an analytic process in our research, not a final product—a common difference between interpretivist and positivist qualitative research. Best practice [136] suggests the codebook should not be reported as we used an interpretivist approach.

Positionality Statement. As researcher identities influence research process and outcomes [137], [138], [139], we briefly describe ours. All members of the team are invested in the values of welcoming and inclusion in cybersecurity, which has motivated our work in this area. One researcher's expertise is in the social dynamics of the computer science community at large and in social change, with a foundation in feminist theory and science and technology studies; all other researchers' expertise is in cybersecurity. All members of our research team currently work in academia. Prior to academia, one researcher worked as a cybersecurity professional for over 5 years and participated in several cybersecurity community organizations. As a team, our analytic perspective is informed by multiple gender identities, a western-centric lens (all team members are currently based in the U.S.), and both white and Asian racial/ethnic experiences.

3.5. Limitations

First, similar to other qualitative studies, we do not claim generality of our results; instead, we document the experiences of cybersecurity organizers whose perspectives and welcoming practices impact many aspiring cybersecurity professionals. To provide a well-rounded perspective, we recruited multiple members across a variety of different types of organizations. We do not use systematic quantifier terminology (e.g., using the term "some" when 2-4 participants express a theme) because our methods are fully qualitative and interpretivist (what Braun and Clarke describe as "Big-Q" [140]). Using strict quantifier terminology can imply theme prevalence tracks real-world prevalence, which we do not assess. Also, as our interviews were not focused on exploring differences between types of organizations, we do not make broad claims about differences and only discuss differences when needed to provide relevant example context. *Second,* while we recruited broadly, almost all participants were US-based (N=15) and three were based in India. We expect many experiences in community culture

will exhibit similarities to those we identified, especially in other WEIRD (Western, Educated, Industrialized, Rich, and Democratic) countries [141], but there are likely critically important differences with non-WEIRD countries, some of which we highlight. This said, most (N=11) represented organizations with global membership, but future work would do well to more intentionally draw on experiences of welcoming within cybersecurity organizations in non-WEIRD regions of the world. *Third,* our results are likely affected by self-selection bias. Even though we explicitly avoid using politically divisive terms in recruitment and interviews, several potential participants chose not to talk with us because they felt the conversation was too politically charged.[1] Furthermore, it is possible some people did not respond due to a lack of welcoming practices to discuss. Therefore, our results should be viewed as enumerating attempts at welcoming practices, but not the full state of welcoming practices across cybersecurity. *Fourth,* our results represent organizers' perspectives, who likely view the community differently from general attendees, particularly newer and more marginalized attendees who often find such communities unwelcoming [1], [6]. We ensure that this context is kept throughout our interpretation and reporting.

4. Participants

Our participants organized academic (N=3) and professional conferences (N=3), university student clubs (N=4), CTF competitions (N=5), and security meetups (N=5). Most held senior executive roles within their organization (N=12), such as President, Founder, or Chair. Others held senior advisory or support roles focused on developing their organization's welcoming culture. Most self-reported as men (N=13), white (N=12), younger than 40 (N=11), and holding a graduate degree (N=10). The overwhelming majority resided in the U.S. (N=15), with three residing in India. In two cases, we interviewed two participants from the same organization. These participants provided unique perspectives: the first due to identity differences that informed different welcoming practices, and the second due to having distinct roles and responsibilities. Table 1 summarizes participants' backgrounds. Interviews took 39 minutes on average.

ID	Role	Community(ies)
P1	Chair	Academic conference
P2	Founder	Student group
P3	Founder	Student group
P4	Founder	Professional conference
P5	President	Student group
P6	Organizer	Professional group
P7	Organizer	Professional group
P8	Event creator	Professional CTF
P9	Founder	Professional conference
P10	Program manager	Professional group
P11	Competition architect	Student CTF
P12	Founder	Student group
P13	Organizer	Student CTF
P14	Co-Chair*	Academic conference
P15	Boardmember	Professional group & conference
P16	Founder	Student CTF
P17	Founder, Organizer	Professional group, Student CTF
P18	Chair	Academic conference

TABLE 1: Participant Roles and Affiliated Communities. *This role focused on developing community culture.

5. Defining Welcoming (RQ1, RQ3.1)

5.1. What Does it Mean to be Welcoming?

Participants defined welcoming as a community where members feel psychological safety, and a community characterized by supportive relationships.

Feeling safe to show up as your full self. Several participants cited psychological safety as essential in a welcoming community. Being able to authentically show up as themselves created an environment conducive for learning and networking without fear of repercussions. This meant it was safe to ask questions, start a conversation with leadership or anyone else, and initiate difficult conversations. P18 said this means "people are willing to listen to the ideas and provide feedback…to be helpful in an empathetic way".

Knowing relationships are supportive by default. Relationships where people could rely on one another are also essential in a welcoming community. Participants want to know other community members would be encouraging through struggles, help them learn new topics, and support their career development. P17 noted "They will remember you, who you are. You'll come in, and it's kind of like…How did that interview go?"

Culture and context impact experience. Different things make different people feel safe and welcome—what may be welcoming for one person might make another uncomfortable. P18 said, "I think [it] will be colored by my lived experiences…it's a gut feeling." This emphasizes welcoming must be customized and customizable. P8 explained this in the context of a CTF with mixed-skill players, "when [we] say welcoming, it's mostly like we want to make sure that [each team] has a good experience of the game, no matter what their final rank is." This CTF needed to do different things for beginners and experienced players.

5.2. Who is welcoming for?

New members. Many participants focused on the newcomer experience and expanding the community as a practice of welcoming. Generally, these definitions could be grouped as "opening the door" or creating new pathways, so anyone interested in joining can do so with minimal effort. A community was welcoming when newcomers could join regardless of their commitment level or their circumstances. "I think communities should be welcoming to anyone who would even want to join, and be very low stakes. You show up as you will, and you enjoy, and you learn on your own accord" (P5). Moreover, participants stated it was important

1. We conducted interviews between February and November of 2025.

that newcomers want to return, as P4 mentioned, "you need to get people to come back and feel welcomed." Event attendance is a useful metric: "the number of people that we have participating month to month is the biggest indicator of... how much that we're welcoming" (P17).

While opening the door may make it easy to walk in, several participants recognized a need to reach out and create pathways into their community. P11 did outreach by "sending emails to other colleges, cyber clubs, be like, 'hey, are you interested? We're trying to accept as many people as possible'... we want anyone that even has the slightest inkling that this could be something they want to do."

A heterogeneous and multicultural community. Some participants also discussed the need to attract and support a diverse group of members beyond those already interested in cybersecurity. A welcoming community should look diverse so people of all backgrounds can "see others they consider to look like themselves, be like themselves, sound like themselves" (P4). P4 further noted, "I don't want to have just the 26-year-old white guy at the conference. I want to have everyone else, and I remember at the very first conference, sitting at the opening ceremonies with everybody sitting in there and realizing that I needed to do much better."

While some groups made active efforts to increase diversity, others were more passive, believing diversity would naturally occur if the community is welcoming. For example, P2 said, "we are not really forcing diversity... as a community, our goal is to reach as many people as possible... we ensure equality of opportunity, and we just hope that diversity happens implicitly."

Everyone. While participants mostly talked about welcoming newcomers and people from diverse backgrounds into the community, one acknowledged that a welcoming environment is not just about newcomers, but is important for people already in the community: "you need to get people to come back and feel welcomed to stay" (P4). Additionally, while welcoming was rarely described explicitly in the context of existing members, the actions leaders described taking (see Section 6) often impact everyone, suggesting existing members can still benefit.

5.3. Why is welcoming necessary in cybersecurity?

Participants often defined welcoming by contrasting it to existing unwelcoming social norms and stereotypes of the security community and broader computing culture. Specifically, participants described norms related to the nerdy boys club atmosphere and a willingness to overlook unprofessional and harmful behaviors by "successful" members.

Cybersecurity is seen as a place for nerds. As discussed in Section 2.4, with the masculinization of computing and cybersecurity, a stereotypical hacker has been viewed as the "computer nerd," an asocial male savant who values mastery of computing technology over interpersonal skills, and had a childhood marked by a "magnetic attraction" to computers [63]. Participants discussed how this nerd-centric community introduced challenges for welcoming newcomers in two ways. First, participants indicated events are often tailored to more-experienced members who know the basics. P16, a CTF organizer, explained this is especially true in the CTF community, which tends to take a "trial-by-fire" approach to beginners: "what we're doing with capture the flag competitions is grab some kid and just throw them into a professional basketball, or whatever professional football game. And you're just like 'good luck'". Participants noted that prioritizing experienced members is not conducive to meaningful learning and often scares off beginners.

Participants also discussed how the technical and adversarial material scared away newcomers. P3 saw this in their student club, where over 300 people joined their club's Discord server, but "a lot of them haven't started getting into [cybersecurity] purely because of how scary it was."

Cybersecurity is seen as a place for bros. The masculine connotations of computing culture and historic acceptability of hostile behavior (see Section 2.4) has led to what some participants described as a "bro culture" in cybersecurity. P15 described the bro culture as one where well-connected men shield each other's toxic behavior, where someone victimized at a conference is afraid to report to anyone in power because "they will protect each other and then destroy people's careers if they're not from that bro culture."

Compounding the masculine stereotypes, there has been a push against initiatives to support marginalized populations, such as women, Black, and Latino/a/x people. This began with technology community leadership reconsidering these efforts to be more welcoming and inclusive [93], [105] and has been supercharged as the new U.S. administration has sought to condemn DEI efforts [106], [107], [108], [109]. P1 mentioned their conference has removed uses of the phrase "DEI" because they "do not want to be anyone's target, politically." Participants reported that groups seen as promoting DEI have had funding reduced, and conferences want to avoid any content that could be viewed as political.

Unprofessional and hostile behavior by some is permitted. Cybersecurity is an inherently adversarial field, and some participants described examples of conferences they had attended building an intentionally adversarial culture. P9 recalled "DEF CON 15 years ago, [with] no cameras, no names, all hacker handles," because using your name could make you a target. Several participants also described examples of explicitly unprofessional behaviors they observed. They described community members treating a professional community as a "dating scene", posting "not safe for work" content to a group's online space, impersonating others in the group's online space, or publicly berating community members. For some participants, tolerating inconsiderate and abrasive people was a necessary evil. P8 mentioned their CTF generally excuses arrogant people, as long as the person is skillful. Particularly in CTFs, which feature a competitive environment, multiple interviewees said some competitors may lash out in frustration about challenges at organizers. Some participants believed organizers must accept this aggressive behavior with grace and not reflect it

back: "if you come in being like, 'my challenge isn't broken, it's *you* that are stupid,' you're gonna piss people off" (P11).

Other participants described more toxic behaviors like harassment being excused. When unprofessional behavior becomes tolerated in the community, it may lead some unscrupulous people to escalate to abject hostility. P14 mentioned hostility has historically been acceptable in academic spaces. She recalled being shocked when entering the community 15 years ago and seeing sexual references and slurs being acceptable, like "conference slides with partially naked women on them... people would be like, what's the big deal?" When she joined her conference, an influential member was credibly accused of sexually assaulting multiple women. Unfortunately, this type of hostility is not uncommon in the cybersecurity community [1], [142].

Participants also described a gendered double-standard. For example, when it came to cases of alcohol abuse—an issue at cybersecurity conferences [143]—if a woman drinks too much at a conference, "they can tell your employer. It will ruin your career. Versus the guys... may get a slap on the wrist if they get drunk, and they do something bad to a female at a conference, but they don't get fired" (P15).

6. Welcoming Practices (RQ2, RQ3.2)

Next, we discuss practices participants use to build a welcoming community and the challenges they faced implementing those practices. We organize practices according to the community aspect they influence, e.g., individual behaviors, relationships between members, and the environment. In each category, practices varied in formality, from explicit rules to implicit norm setting. Throughout, we discuss challenges participants faced implementing practices. However, we do not make claims regarding practice efficacy.

6.1. Shaping Member Behaviors

Many participants discussed building a welcoming community by encouraging individuals to adopt positive, welcoming behaviors and discouraging unwelcoming behaviors.

Codes of conduct provide formal requirements for members and signal a community's priorities. Codes of conduct are inherently a formal practice as they put in writing rules community members are expected to follow. Participants described two common roles a code of conduct should play: to guide participant behaviors through positive example, and guide enforcement actions should their behavior fall outside the acceptable range. As P5 stated, a code of conduct tells members "how they should treat one another... defining what appropriate social behavior entails." Codes of conduct may also signal that leaders have considered how to make the environment welcoming and safe. As P15 stated, "if they have a code of conduct, I will be more inclined to learn more about the conference, and I may attend it." An effective code of conduct must also be enforceable. P7 mentioned a community they were formerly part of splintered after leaders did not properly enforce the code of conduct: "that wasn't for lack of having a code of conduct...I think part of that art is also how it's enforced." P15 explained that conferences without an enforceable code of conduct "push the accountability onto the attendees" and support a narrative of bad actors instead of toxic culture.

Challenge: Believing creating rules hinders welcoming. Some participants expressed worry that codes of conduct may be too legalistic or that creating rules might conflict with the welcoming atmosphere they sought to create. As P2 described, "we don't really have a very tight set of rules. Because in the end, we just wanted to be as open as possible. Discuss whatever you want, as long as you're not really bothering anyone." We note that P2's group was new, and so they were more focused on growing and establishing their community than creating administrative rules. Other participants sought to boost participation by making meeting attendance mandatory or requiring interested parties to "apply" for acceptance to the community. Creating a sense of exclusivity may boost engagement within the community, though it also meant creating a threat of expulsion for anyone not meeting the minimum requirements. P5 noted that after their club required attendance, "it brought in members who would regularly go to every meeting," which has been a positive change for their club, even though they had to kick out "a few members" for insufficient attendance.

Challenge: Maintaining codes of conduct can be difficult. Organizers should regularly revisit the code of conduct and make revisions as needed to ensure it continues to serve the community's needs. P15's community annually revised their code of conduct "based on things that have happened in political nature... or anything from the results of surveys." If the code of conduct does not remain salient to the community, it may be forgotten, as happened to P17 who was unaware a former organizer's code of conduct remained on a third-party website. P17 thought deeply about making their community welcoming, though the code of conduct became a vestige after its creator left the community.

Organizers rarely reported conflict except in online spaces. While we asked participants to provide examples to demonstrate their conflict resolution process, most said they could not think of examples. We note this absence of examples should not be interpreted as an absence of conflict, as prior research [1], [6] and anecdotal evidence have shown conflict exists across the cybersecurity community. Rather, conflict is likely not being escalated to organizers, a common issue for communities in other domains [144], [145]. The one category of conflict participants discussed was offensive behaviors in online forums, primarily among communities with a significant online presence. P16 mentioned a frequent event where a "new person gets frustrated and is screaming at someone that's trying to help them." Organizers often resorted to banning accounts to remove hostile individuals.

Organizers shape behavior informally by rewarding good behavior. Beyond the formal code of conduct and its enforcement, several participants discussed ways to incentivize what they viewed as good behavior via informal interactions with community members. For example, P12

described liking or responding to "good" content on their community Discord server: "I would be like 'yes, more of that,' and [the community member] would get more attention" and ignoring "bad" content or privately messaging the poster to say "hey bro, knock it off." P12 mentioned structuring their community's Discord server to prioritize members who regularly helped others during meetings and events. These students were given the "helper" role, which prioritized their comments and gave them access to additional resources to show that, in P12's organization, "helping other people is the thing that gets you the furthest."

As another example, some participants supported first-time speakers through optional mentorship programs or required all presenters to do a practice session prior to speaking at their conferences: "we made every presenter give a talk, and so if there was something that felt really off attitude-wise, we had a chance to address it" (P9). This had the dual benefit of providing support to newer speakers to help them feel more prepared, while also giving the organizers the opportunity to set norms for presentations. For example, organizers described a focus on cutting things other community members might find unwelcoming.

Organizers set community norms by modeling acceptable behavior. Several participants described leveraging their position within the community to demonstrate welcoming behaviors as an example to follow. Foremost, leaders ensured their actions supported a psychologically safe environment. For example, P6 mentioned "I become an extraverted introvert in some fashion, because I need to make other people comfortable." P4 ensures their conference organizers are centering attendees and not developing egos. This stems from their experience at other conferences, where "volunteers try to get an attitude and make it about themselves…we need to disappear into the background. The attendees and the speakers are far more important". Being approachable and proactively introducing people also maintains psychological safety. P7 recalled introductions helping her overcome nervousness and integrate when she was new: "I walk in [to] a room full of dudes, to be honest, and all of them kind of collecting towards the beer keg, in a way, and I was scared initially…but it helped that I had colleagues with me who actually introduced me to the group." Now an organizer, she begins each monthly meetup by mingling with other attendees, making sure to introduce herself to other women to make them feel welcome.

Organizers act as a lightning rod, shielding members. Some participants mentioned engaging with people complaining or exhibiting asocial behaviors, putting themselves in an uncomfortable position to shield other members from having a bad experience. P11 noted, "you're gonna get people complaining…being like, hey…this challenge sucks." When a person's behavior challenges others' ability to participate, banning may be necessary. Participants whose groups had a significant online presence discussed using "the ban hammer" (P16). P12 mentioned there should be "a core inner group where there's trust between the members" who can decide whether a person's behavior warrants banning.

6.2. Supporting Relationship Development

Broadening their focus beyond the individual, several participants described community building practices targeted specifically at helping community members develop relationships with others in the organization.

Formal mentoring programs. Perhaps the most formal relationship development practice participants described was mentorship programs. P14 noted that in an academic conference setting, making a junior-senior connection can be daunting: "approaching a senior researcher to ask them a question about their paper when they're in conversation with people that they know is not easy to do for a junior researcher." To solve this problem, they established speed mentoring, which creates a social context where these conversations are welcome. Another participant mentioned their student club evaluates each newcomer's experience level so they can pair more- and less-experienced newcomers for onboarding activities. Since onboarding education would be boring for the more-experienced newcomer, P5 said, "they end up helping out in the new member education process, and like kind of mentoring the other new members".

Challenge: Senior members might not believe they can mentor people from different backgrounds. Participation in mentoring programs is often voluntary. Therefore, mentors must feel they have relevant skills and experiences so they will feel confident to volunteer their service. One participant noted seeing some mentors from majority groups feel they do not have the experience required to mentor someone from a minority group. This hesitation could result in fewer mentors in the program for members from minority groups, who often are already less likely to have mentors in the cybersecurity community overall [6]. P14 offered a pithy response to any mentor in this situation: "here's what you do: you just treat [the mentees] like scientists."

Integrate newcomers with informal mentorship. Similar to formal mentoring, some participants described less formal practices to support newcomer involvement by pairing newcomers with more senior members of the community. For example, structuring activities so new and old community members work on a problem together, facilitating discussion between new and old members, and informal newcomer introductions. Some participants announced this practice's purpose to clearly articulate the goal of the pairings. P5 explained, "in the first few meetings of every semester, we have these collaborative activities [simple CTF challenges] where we randomly put…returning members and new members…together". This is similar to a mentorship program, though not as formal as participants were not required to sign up ahead of time. Others chose not to center this goal of relationship building, instead allowing relationships to develop naturally from the forced proximity.

Fostering ongoing connections to promote unity and temper adversarial responses. Several organizers mentioned practices that support connections and help *all* community members participate, not just newcomers. Organizers structured activities to encourage socializing, made the

community feel smaller by hosting workshops and small group discussions, and provided topics for discussion. P6 emphasized keeping the atmosphere light at the start of each event to help people get to know each other and avoid adversarial conversations. This enables more considerate, but still spirited debate later on because "the fact that people are very familiar with each other's faces gives them the ability to be more... not confrontational, but just get in that spirit of debate, because as you can imagine, [in] hackerspace... we're no strangers to controversy or debate."

6.3. Setting the Environment

Finally, participants discussed practices to design an environment that encouraged community development and made all participants feel welcomed.

Identify and address challenges to participation early. Creating a welcoming environment for everyone requires proactively identifying where friction might prevent some from participating. For example, P4 explained that working with accessibility specialists can identify hidden barriers, like "lights that are too bright, sounds that are too loud, anything that's blinking." Some participants emphasized the importance of providing childcare stipends and accommodating dietary restrictions to ensure everyone can participate. As P7 said, "we also try and cater to different audiences... in terms of food, in terms of accommodations that we can do as well". After doing background work to make the community more accessible, participants expressed it is beneficial to promote the work done. For example, P14 said advertising family stipend availability "signals to [others] that you are a certain kind of community that is aware that sometimes people need to look after young people or older people."

Challenge: funding sources impose restrictions. Funding sources may restrict how funds may be used. As P14 mentioned, "private foundations are more likely to let you pay for childcare, for example. NSF will not let you do that." Organizational labor can maximize the use of each source.

Crafting the physical space to help people connect. A physical space's design and layout can implicitly affect how people will (or will not) interact inside it [146]. A few participants described making physical layout changes to encourage connection. P9 rearranged gathering spaces to promote socializing: "every night was a different part of the hotel with a different place. We wanted people to intentionally mix and mingle and talk to different folks."Others created designated areas and times for off-topic events to help members create connections about topics beyond the relevant subject matter. P15 created two spaces for a networking night: "one was a karaoke place, so for those that are a little bit more extravert... and then in the other room there was a bunch of games on each table that people can do, and some of them you could do on your own... it was basically trying to ensure that no matter what your background is, you feel accepted."

Choose sponsors carefully and monitor sponsor events. Vetting sponsors is a more informal way of ensuring an organization embodies its values. Some participants mentioned carefully vetting sponsors, since accepting support from another group is tacit endorsement of their values. As P15 stated, "if we do take funds, we do a check to see if they do practice DEI, so if they have DEI policies, we'll be okay with it." Participants said it is important to vet any sponsor that wishes to host an off-site event, since mishandled incidents will still reflect poorly on the main conference. P15 explained that organizers should "make sure that if there's going to be a networking event that will be happening at your conference, to ensure that the [sponsor] company... is going to ensure the safety of the attendees." Others mentioned sponsors can participate in the community in addition to financial support. P17 mentioned "for the companies that sponsor, we want more than just money... we want you to come be a part of this [event]." Sponsors can provide knowledge and guidance, especially to novices, as in P17's community's CTF.

Create spaces where participants feel represented. Related to welcoming is the concept of safe spaces, which are supportive environments free from bias, where participants feel represented [147]. Building these spaces was a central focus for some participants. P15's organization's goal was specifically to create a safe space for underrepresented groups in cybersecurity, P13 had hosted an event for women in cybersecurity, and P14 had previously held a position to create safe spaces. P4 wanted to create a space where people are "able to see others that they consider to look like themselves, be like themselves, sound like themselves."

Several participants explained that an important step in creating safe spaces is ensuring leadership has the knowledge and lived experiences required to understand what makes a space safe for a particular identity group. P15 mentioned having neurodivergent board members helped them create safer environments for neurodivergent attendees: "it really does help when you have people from all different backgrounds on the board... because everyone kind of just gets each other." P15 also described efforts to recruit board members from organizations primarily serving Black cybersecurity professionals to ensure more diverse leadership. Beyond the knowledge diverse leadership brings, P15 explained that recruiting from organizations serving underrepresented groups signaled to those other groups that P15's organization was welcoming to diverse identities, saying "they also told their members that, hey, there's this conference that's trying to learn, trying to get better."

Challenge: Hard to create diversity when leadership roles filled by known colleagues. An ideal world might see people selected to leadership based only on merit. In reality, participants said leaders often fill roles with people they know and trust. This may hinder efforts to diversify boards and committees. P18 recounted a moment when a well-qualified person they nominated for a program committee was not selected because the track chairs "just don't know him."

Intentionally invite historically excluded communities. Multiple participants described focusing on recruiting people from organizations associated with historically excluded

communities. They saw two benefits: 1) people from these targeted organizations feel explicitly welcomed, and 2) this signals to others that everyone is welcome. As P4 stated, "one of the things that I really try to do, is to find all these different groups, and to proactively invite them in and tell them, we want you here, we want you to be a part of this." However, signaling can backfire when it is interpreted as an empty gesture or something that draws attention to one's status as "other." P16 recalled one such negative experience at a conference that was attempting to show support for immigrants in the U.S.: "the organizers, I think meaning well by this, said, 'Hey, can all of the immigrants in the audience stand up' and I stood up, and there is a [message] like 'we support you, blah blah,' and I have never felt so pointed out. It was a very uncomfortable experience for me."

Challenge: Diversity not acknowledged by everyone as important for science. One participant mentioned the misconception that diversity is "extra" rather than seeing it as a fundamental component of good science. Believing diversity is extra means we may discard it when inconvenient, but then we could be doing junk science. They invoked an example where "if you were to write out like in a paper, 'we tested how this system works on white people, and it works fine, and we haven't tested it on anybody else.'... I mean, globally, that's a pretty limited subset." If we want to build knowledge and systems that are true of everyone and work for everyone, we must include everyone.

Create beginner-friendly on-ramps into cybersec orgs for newcomers. Many participants who led CTFs and student groups described creating beginner-friendly materials to onboard newcomers and make cybersecurity approachable. This practice specifically sought to combat the common emphasis on experienced members (see Section 5.3). P2 and P3 created engaging materials on web security fundamentals so newcomers "don't get bored of it, because it's not like a lecture where you sit and listen." Participants also assumed newcomers have no technical background, as P13 explained, "If it's required that you know how to use a shell, then that's not an equal opportunity. There are kids around the world who learn programming, and they don't know what a terminal or a shell is, because somebody taught them through an IDE." Reducing the barrier to entry and creating onboarding materials signals to novices that they are welcome and gives them the tools to begin participating in the community.

Create infrastructure to solicit and respond to community input. Most participants actively solicited feedback from their community members, whether in general or for specific policies. A few participants preferred the town hall format for soliciting feedback, as it evoked an egalitarian atmosphere where anyone could speak up. P14 explained, "even if... it was your first time in the room, there's no hierarchy, like you are just like, 'hey, I have a thing to say.'"

DEI backlash changes words, not practices. Though no participants reported changes to their welcoming practices in response to DEI backlash, some were more mindful of words they used to avoid appearing "woke." P1 mentioned "if we don't write 'DEI' on the website, then that is sort of the trade-off that we've decided we're willing to make. We're still doing all the other things behind the scenes, in the ways that we were before [or] even more actively." The labels they used for these practices were less important than their effects: "If you are inclusive, you're doing DEI regardless of whether the label is there" (P13). The pressure to remove DEI terms appeared external and no participants reported their community members pushing back against welcoming practices or related examples of conflict. However, some participants reported the DEI backlash appeared to result in reduced funding for their organization. P15, who runs a conference focused on advancing DEI in computing, noted funding "has been slowing down... we didn't think that we'd be able to have a conference this year."

Some participants believed a welcoming community should develop organically. Finally, some participants stressed that a healthy community should function without constant active management from leadership. This could mean the community handles some conflict without needing leaders involved, and members grow the community or build new parts without pressure from leadership. P17 described witnessing a moment of community connection at their CTF: "we had these really top-notch folks... they had, like, twice the points in the CTF. And at a certain point, they just stopped. And they got up, and they walked around, and they were helping people. And I was like, this is amazing. This is what community is." P18 echoed that while organizers can "create the substrate" for community, it is the people within the community who create welcoming environments. They emphasized that even though large communities tend to cluster into smaller groups, welcoming must be community-wide: "to grow a community, valuing others who are providing feedback while being strict in what you believe in is a fine balance that each community has to navigate."

7. Discussion

7.1. Is Welcoming Necessary in Cybersecurity?

Given our focus on *welcoming*, a skeptic will ask, *is welcoming actually necessary in cybersecurity?* Taking this counterargument seriously, we put our results in conversation with the cultural and historical context of cybersecurity and hacker ethos (Section 2.1) to illustrate how cultural change centering *welcoming* is necessary to address long-standing issues around recruitment and retention.Through our results, we see cybersecurity's cultural norms and values (e.g., obsessive focus on programming, commitment to the concept of meritocracy, and adversarial thinking's centrality) can be weaponized to uphold an unwelcoming culture.

Take the belief in meritocracy—the concept on its face seems like it should contribute to a welcoming culture (thus making efforts towards welcoming unnecessary); however, this idea ends up being leveraged towards unwelcoming and exclusionary outcomes in practice.For example, our participants discussed how some hacker communities insist on "trials-by-fire" and acts of commitment that segregate

newcomers and test their ability to withstand the community's hostile environment (Section 5.3), ultimately ignoring broader societal circumstances that systemically disadvantage people from marginalized communities (Section 6.3).

Moreover, having adversariality as a core value introduces paradoxical cultural artifacts for cybersecurity: constantly being alert and on edge because threats are everywhere engenders vigilance that is helpful for practitioners to stay sharp in their work, but this vigilance is often at odds with feelings of safety and comfort. In the name of adversarial thinking, we encourage cybersecurity community members to think creatively and divergently, to learn to take on the perspective of bad-actors and attackers. We create sandboxes where lock-picking and cheating are games—games that can be a blast! The issue our participants pointed out is that not everyone understands when and where the game should end, when hostility and conflict cross a line. Power imbalances, particularly historical and systemic imbalances, can exacerbate conflicts and hostility [148], [149], [150]. In the context of adversarial games, it is possible what seems like good-natured play to a person with more-power is harmful or dangerous to a person with less-power. Adversariality's cultural paradox emerges throughout our findings. We see this in the ways participants felt the need to act as a lightning rod to divert hostility away from others (Section 6.1), *and* in their frustrations around how unprofessional and hostile behavior is tolerated in cybersecurity (Section 5.3).

From the hacker ethic to adversarial thinking, there are tensions in cybersecurity culture's core contributing to unwelcoming and unjust outcomes. Without addressing hostility through counter-cultural values like welcoming, exclusion will persist and make it difficult to recruit and retain a diverse workforce. We defined welcoming as a core community culture feature signaling members are wanted, will be included, and feel they belong. Moreover, safety is an essential feature of belonging and inclusion [1], [116]. While adversariality's cultural paradox speaks to the complex relationship between *security* and *safety*, these concepts are dependent upon one another. Building on transnational feminist principles (e.g., [111], [122], [151], [152]), we understand safety as freedom from oppression (particularly understanding that oppression has different shapes in different contexts). Ideally, security is something we undertake to enable safety, rather than an exercise in hostility in and of itself. Critically, the transnational, intersectional perspective on freedom from oppression is not necessarily at odds with the hacker's ethos. Thus, focusing on concepts like welcoming and safety in cybersecurity provide a path to balance cybersecurity's complex and paradoxical core cultural tenets like adversarial thinking while pointing towards ways to counteract ongoing ambient hostility that negatively impacts recruitment and retention for newcomers and experts alike.

7.2. Building on Welcoming Practices

Participants leveraged welcoming practices to address cybersecurity culture's core tensions. We contextualize these practices within the broader literature to identify which may be particularly impactful, and other opportunities that exist.

Rules work—but often indirectly, and only with structure. While most participants created codes of conduct without disciplinary mechanisms, they were effective at signaling community intentions (Section 6.1). Some participants even mentioned how strict rules can impede welcoming. These beliefs are in line with prior literature studying rules' impact on organizational diversity and retention. The use of discipline can result in community harm as organizers may be incentivized to avoid conflict and its associated effort [97] or they can lull organizers into a false sense of security [144] while victims do not report for fear of retaliation [145].

Studies in other fields have found if communities want rules to effect change beyond virtue signaling, additional community structures are needed. One option is the establishment of an ombudsman, an individual or group outside the organization who can receive confidential feedback. Ombudsmen can have a positive effect on organization diversity and retention, allowing members to be heard and ensure the organizers are aware of problems [92]. Furthermore, if communities wish to strengthen community norms beyond codes of conduct, inclusion and bystander training with organizers has shown to be effective [92]. These programs position organizers as positive community forces and help them know how to best support marginalized members.

Mentorship is important, but should be formal and for everyone. Our participants' emphasis on building relationships through mentorship (Section 6.2) fits prior literature's recommendations. If done well, mentoring opens up resources and opportunities for mentees and mentors [92]. However, many participants emphasized informal mentorship development, which, unfortunately, rarely leads to personal and committed cross-race or -gender mentoring [153], disproportionately isolating those from historically excluded communities. In our findings, we see this through the emphasis on bro cultures and the (albeit well-intentioned) discomfort senior members have with mentoring junior members of different races or genders. To address this, prior work prioritizes formal mentoring and suggests mentor/mentee pairing by interest to build bonds [154]. Additionally, participants most often discussed mentoring newcomers. While this is essential, organizers should consider mentoring at all stages to avoid burnout and support career development [92].

Hackers are people too... and people have complicated lives. When considering shaping the organization's environment to be welcoming (Section 6.3), our participants recognized their members have a variety of needs and outside circumstances to account for in making their environments more accessible (e.g., mobility, communication, diet, religious practices, care-taking, etc.). Determining all the access needs in a given community can be complicated, so it is best to understand the specific needs of a given community and seek out guidance on good-practices. Further, it is important organizers not only provide and advertise resources to support work-life balance and accessibility, but actively encourage and normalize their use. Otherwise, members

may forego them to avoid looking weak among the broader hacker culture [155]. Considering burnout is a common challenge (worsened by the hacker stereotype's singular devotion to cybersecurity), work-life balance is essential to create a community where people feel welcome [156].

Acknowledgments

Many thanks to our participants for their contribution to this work and to their cybersecurity communities. We are grateful for the anonymous reviewers who provided helpful comments on this paper's drafts. We thank Chloé Messdaghi, Jordan Weins, and Amira Chhaiouine for their help recruiting. This project was supported by a gift from Google and NSF grant CNS-2440353.

References

[1] S. Katcher, L. Wang, C. Yang, C. Messdaghi, M. L. Mazurek, M. Chetty, K. R. Fulton, and D. Votipka, "A survey of cybersecurity Professionals' perceptions and experiences of safety and belonging in the community," in *Twentieth Symposium on Usable Privacy and Security (SOUPS)*, Aug. 2024.

[2] D. A. Garvin, A. C. Edmondson, and F. Gino, "Is yours a learning organization?" *Harvard business review*, vol. 86, no. 3, p. 109, 2008.

[3] "What is psychological safety at work? Here's how to start creating it," 2024. [Online]. Available: https://www.apa.org/topics/healthy-workplaces/psychological-safety

[4] "What is psychological safety?" McKinsey & Company, Jul. 2023. [Online]. Available: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-psychological-safety#/

[5] M. Blanding, "In Tough Times, Psychological Safety Is a Requirement, Not a Luxury," *Harvard Business Review*, Nov. 2025. [Online]. Available: https://hbr.org/2025/11/in-tough-times-psychological-safety-is-a-requirement-not-a-luxury

[6] K. R. Fulton, S. Katcher, K. Song, M. Chetty, M. L. Mazurek, C. Messdaghi, and D. Votipka, "Vulnerability discovery for all: Experiences of marginalization in vulnerability discovery," in *Proceedings of the 44th IEEE Symposium on Security and Privacy*, ser. IEEE S&P '23, 2023.

[7] D. CON, "Def con hacking conference - frequently asked questions," https://defcon.org/html/links/dc-faq/dc-faq.html, (Accessed 06-11-2026).

[8] J. S. Granick, M. Hofmann, and R. Jeschke, "Mit students gagged by federal court judge," https://www.eff.org/press/archives/2008/08/09, September 2008.

[9] C. Pellerin, "Three teams earn prizes in darpa cyber grand challenge," https://www.war.gov/News/News-Stories/Article/Article/906931/three-teams-earn-prizes-in-darpa-cyber-grand-challenge/, April 2016.

[10] J. Uchill, "Hackers breach dozens of voting machines brought to conference," https://thehill.com/policy/cybersecurity/344488-hackers-break-into-voting-machines-in-minutes-at-hacking-competition/, July 2017.

[11] J. Moss, D. Lute, J. Braun, H. Hursti, S. Ramsay, and J. Gilligan, "Voting machine security," https://www.c-span.org/program/public-affairs-event/voting-machine-security/488780, October 2017.

[12] S. Korber, "Cyberteams duke it out in the world series of hacking," https://www.cnbc.com/2013/11/08/defcon-capture-the-flag-competition-is-only-for-top-hackers.html, November 2013.

[13] D. Bullock, "Inside the World's Most Hostile Network," *Wired*, Aug. 2009. [Online]. Available: https://www.wired.com/2009/08/inside-the-worlds-most-hostile-network/

[14] Doc, "Wall of Sheep," Nov. 2022. [Online]. Available: https://www.phvillage.io/pages/wall-of-sheep/

[15] J. Sakellariadis, "For U.S. officials, the world's largest hacking conference isn't all fun and games," Aug. 2023. [Online]. Available: https://www.politico.com/news/2023/08/12/u-s-officials-def-con-hacking-conference-00110946

[16] "Def con conference transparency report," DEF CON. [Online]. Available: https://defcon.org/html/links/dc-transparency.html

[17] "Conference code of conduct," DEF CON. [Online]. Available: https://defcon.org/html/links/dc-code-of-conduct.html

[18] C. Faife, "Def Con banned a social engineering star — now he's suing," Aug. 2022. [Online]. Available: https://www.theverge.com/2022/8/18/23311573/chris-hadnagy-social-engineering-def-con-ban-lawsuit-jeff-moss

[19] E. Volokh, "Defamation Lawsuit Against Def Con Cybersecurity Conference Dismissed," May 2025. [Online]. Available: https://reason.com/volokh/2025/05/13/defamation-lawsuit-against-def-con-cybersecurity-conference-dismissed/

[20] C. Jones, "Chris Hadnagy allegations revealed in trial filings," Feb. 2025. [Online]. Available: https://www.theregister.com/security/2025/02/25/chris-hadnagy-allegations-revealed-in-trial-filings/453620

[21] Emma, "Announcing the new women-only hacking community: Hackerher network," https://www.bugcrowd.com/blog/announcing-the-new-women-only-hacking-community-hackerher-network/, Bugcrowd, March 2025.

[22] N. I. for Cybersecurity Careers and Studies, "Cybersecurity education and training assistant program," https://niccs.cisa.gov/cybersecurity-career-resources/cybersecurity-education-and-training-assistance-program, US Cybersecurity and Infrastructure Security Agency, (Accessed 06-11-2026).

[23] N. I. for Cybersecurity Education, "National initiative for cybersecurity education workforce framework for cybersecurity," https://niccs.cisa.gov/tools/nice-framework, US Cybersecurity and Infrastructure Security Agency, (Accessed 06-11-2026).

[24] L. Quintana, "Hack your way to a new career in cybersecurity: Cisco networking academy offers new ethical hacker course," https://blogs.cisco.com/learning/hack-your-way-to-a-new-career-in-cybersecurity, Cisco, Oct. 2023, (Accessed 06-11-2026).

[25] F. S. Legislature, "The florida center for cybersecurity - florida statute 1004.444," https://www.leg.state.fl.us/statutes/index.cfm?mode=View%20Statutes&SubMenu=1&App_mode=Display_Statute&Search_String=1004.444&URL=1000-1099/1004/Sections/1004.444.html, Florida State Legislature, 2025, (Accessed 06-11-2026).

[26] O. C. R. Insitute, "Ohio cyber range institute: Unlocking potential, securing the future," https://www.ohiocyberrangeinstitute.org/, Ohio Cyber Range Institute, (Accessed 06-11-2026).

[27] T. Trevethan and G. Williams, "The time is now to secure the future," https://www.paloaltonetworks.com/blog/2023/10/secure-the-future/, PaloAlto Networks, Oct. 2023, (Accessed 06-11-2026).

[28] $(ICS2)^2$, "Cybersecurity workforce study," www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx, $(ICS2)^2$, Tech. Rep., August 2018.

[29] A. Chavarria, "2022 isc2 cybersecurity workforce report," https://training.totalcyber.com/2022-isc2-cybersecurity-workforce-report/, November 2022.

[30] ISC2, "Isc2 cybersecurity workforce study 2023," https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e, 2023.

[31] $(ICS2)^2$, "Global cybersecurity workforce prepares for an ai-driven world," https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/research/2024-ISC2-WFS.pdf, $(ICS2)^2$, Tech. Rep., August 2018.

[32] ISC2, "Isc2 cybersecurity workforce study 2025," https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study, 2025.

[33] ISACA, "The state of cybersecurity 2025: Global update on workforce, resources and operations," https://www.isaca.org/resources/reports/state-of-cybersecurity-2025, September 2025.

[34] B. C. Holtom, T. R. Mitchell, T. W. Lee, and M. B. Eberly, "Turnover and retention research: A glance at the past, a closer review of the present, and a venture into the future," *Academy of Management Annals*, vol. 2, no. 1, pp. 231–274, 2008.

[35] BugCrowd, "Inside the mind of a hacker: The human-augmented intelligence era," BugCrowd, 2026, (Accessed 06-03-2026). [Online]. Available: https://www.bugcrowd.com/wp-content/uploads/2026/01/Inside-the-Mind-of-a-Hacker-2026.pdf

[36] ——, "Inside the mind of a hacker 2020," BugCrowd, 2020, (Accessed 07-21-2020). [Online]. Available: https://itmoah.bugcrowd.com

[37] HackerOne, "The 2020 hacker report," https://www.hackerone.com/sites/default/files/2020-04/the-2020-hacker-report.pdf, HackerOne, San Francisco, California, Tech. Rep., December 2020.

[38] D. Votipka, R. Stevens, E. M. Redmiles, J. Hu, and M. L. Mazurek, "Hackers vs. testers: A comparison of software vulnerability discovery processes," in *Proceedings of the 39th IEEE Symposium on Security and Privacy*, ser. IEEE S&P '18, 2018.

[39] F. Hermans and A. Schlesinger, "A case for feminism in programming language design," in *Proceedings of the 2024 ACM SIGPLAN International Symposium on New Ideas, New Paradigms, and Reflections on Programming and Software*, ser. Onward! '24, vol. 12. ACM, Oct. 2024, pp. 205–222.

[40] S. Turkle, *The Second Self*, twentieth anniversary ed. ed. Cambridge, Massachusetts: MIT Press, 2005.

[41] J. Weizenbaum, *Computer Power and Human Reason*. San Francisco: Freeman, 1976, literaturangaben.

[42] P. Himanen, *The Hacker Ethic, and the Spirit of the Information Age*. New York: Random House, 2001.

[43] N. Ensmenger, ""beards, sandals, and other signs of rugged individualism": Masculine culture within the computing professions," *Osiris*, vol. 30, no. 1, pp. 38–65, Jan. 2015.

[44] S. Levy, *Hackers: Heroes of the Computer Revolution*, 25th ed. Sebastopol, Calif.: O'Reilly Media, 2010, description based on print version record. - Includes bibliographical references (p. 395-398) and index.

[45] J. Metcalf, E. Moss, and d. boyd, "Owning ethics: Corporate logics, silicon valley, and the institutionalization of ethics," *Social Research: An International Quarterly*, vol. 86, no. 2, pp. 449–476, Jun. 2019.

[46] C. C. Perez, *Invisible Women: Data Bias in a World Designed for Men*. Abrams Press, Mar. 2019.

[47] M. Blair-Loy and E. A. Cech, *Misconceiving Merit*. University of Chicago Press, 2022.

[48] R. Eglash, "Race, Sex, and Nerds: From Black Geeks to Asian American Hipsters," *Social Text*, vol. 20, no. 2, pp. 49–64, 2002. [Online]. Available: https://muse.jhu.edu/pub/4/article/31927

[49] A. H. Amsden and J. C. Clark, *Software Entrepreneurship among the Urban Poor: Could Bill Gates Have Succeeded If He Were Black?... Or Impoverished*. Cambridge, MA: MIT Press, 1999, pp. 213–234.

[50] Z. Cullen and R. Perez-Truglia, "The old boys' club: Schmoozing and the gender gap," *American Economic Review*, vol. 113, no. 7, pp. 1703–1740, Jul. 2023.

[51] V. Michelman, J. Price, and S. D. Zimmerman, "Old boys' clubs and upward mobility among the educational elite," *The Quarterly Journal of Economics*, vol. 137, no. 2, pp. 845–909, Dec. 2021.

[52] S. McDonald, "What's in the "old boys" network? accessing social capital in gendered and racialized networks," *Social Networks*, vol. 33, no. 4, pp. 317–330, Oct. 2011.

[53] J. Abbate, *The Pleasure Paradox: Bridging the Gap between Popular Images of Computingand Women's Historical Experiences*. John Wiley & Sons, Jun. 2010, ch. 10.

[54] C. Dunbar-Hester, ""Freedom from jobs" or learning to love to labor? diversity advocacy and working imaginaries in open technology projects," *Teknokultura. Revista de Cultura Digital y Movimientos Sociales*, vol. 13, no. 2, pp. 541–566, Nov. 2016.

[55] V. Ojha, C. Perdriau, B. Lagesse, and C. M. Lewis, "Computing specializations: Perceptions of AI and cybersecurity among CS students," in *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1*, ser. SIGCSE 2023. ACM, Mar. 2023, pp. 966–972.

[56] T. Oakley Browne and E. Pardede, "A systematic review on adversarial thinking in cyber security education: Themes and potential frameworks," *Computers & Security*, vol. 163, p. 104803, Apr. 2026.

[57] R. Derbyshire, B. Green, and D. Hutchison, ""Talking a different Language": Anticipating adversary attack cost for cyber risk assessment," *Computers & Security*, vol. 103, p. 102163, Apr. 2021.

[58] "Adversarial," [Oxford], 2011, "Oxford Reference Online Premium.". - Title from home page (viewed Apr. 8, 2011).

[59] T. Dimkov, W. Pieters, and P. Hartel, "Training students to steal: A practical assignment in computer security education," in *Proceedings of the 42nd ACM technical symposium on Computer science education*, ser. SIGCSE '11. ACM, Mar. 2011, pp. 21–26.

[60] G. Conti and J. Caroland, "Embracing the kobayashi maru: Why you should teach your students to cheat," *IEEE Security & Privacy Magazine*, vol. 9, no. 4, pp. 48–51, Jul. 2011.

[61] J. Mirkovic and P. A. H. Peterson, "Class Capture-the-Flag exercises," in *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*. San Diego, CA: USENIX Association, Aug. 2014. [Online]. Available: https://www.usenix.org/conference/3gse14/summit-program/presentation/mirkovic

[62] S. Roschke, C. Willems, and C. Meinel, "A security laboratory for CTF scenarios and teaching IDS," in *2010 2nd International Conference on Education Technology and Computer*. IEEE, Jun. 2010, pp. V1–433–V1–437.

[63] J. Margolis and A. Fisher, *Unlocking the Clubhouse: Women in Computing*. Cambridge, Mass: MIT Press, 2002.

[64] T. Camp, "The incredible shrinking pipeline," *ACM SIGCSE Bulletin*, vol. 34, no. 2, pp. 129–134, Jun. 2002.

[65] J. Cuny and W. Aspray, "Recruitment and retention of women graduate students in computer science and engineering," *Washington, DC: Computing Research Association*, 2001.

[66] K. Mahony and B. V. Toen, "Mathematical formalism as a means of occupational closure in computing — why 'hard' computing tends to exclude women," *Gender and Education*, vol. 2, no. 3, pp. 319–331, Jan. 1990.

[67] K. A. Frenkel, "Women and computing," *Communications of the ACM*, vol. 33, no. 11, pp. 34–46, Nov. 1990.

[68] D. Gürer and T. Camp, "An ACM-W literature review on women in computing," *ACM SIGCSE Bulletin*, vol. 34, no. 2, pp. 121–127, Jun. 2002.

[69] R. Yamaguchi and J. D. Burge, "Intersectionality in the narratives of black women in computing through the education and workforce pipeline," *Journal for Multicultural Education*, vol. 13, no. 3, pp. 215–235, Aug. 2019.

[70] A. T. Wynn and S. J. Correll, "Puncturing the pipeline: Do technology companies alienate women in recruiting sessions?" *Social Studies of Science*, vol. 48, no. 1, pp. 149–164, Feb. 2018.

[71] M. desJardins, R. Libeskind-Hadas, M. Balazinska, S. Hambrusch, C. Isbell, and M. Medard, "Growing and diversifying the domestic graduate pipeline," Jun. 2021.

[72] J. Margolis, *Stuck in the Shallow End: Education, Race, and Computing*. Cambridge, Mass: MIT Press, 2008.

[73] A. H. Tapia and L. Kvasny, "Recruitment is never enough: Retention of women and minorities in the IT workplace," in *Proceedings of the 2004 SIGMIS Conference on Computer Personnel Research: Careers, Culture, and Ethics in a Networked Environment*, ser. SIGMAS CPR '04. New York, NY, USA: ACM, 2004, pp. 84–91.

[74] R. E. Ladner and M. Israel, ""For all" in "computer science for all"," *Communications of the ACM*, vol. 59, no. 9, pp. 26–28, Aug. 2016.

[75] M. Holanda, A. Lima, L. Silva, M. Mitzi, E. Bernardes, J. Gondim, A. P. F. Araúdo, C. Chamon, D. Da Silva, and M. E. Walter, "Women in cybersecurity: A literature mapping (2010-2024)," in *2025 IEEE Frontiers in Education Conference (FIE)*. IEEE, Nov. 2025, pp. 1–9.

[76] E. Selman-Housein and B. Plancher, "Improving the representation of undergraduate women in cybersecurity: A literature review," in *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1*, ser. SIGCSE TS 2025. ACM, Feb. 2025, pp. 1043–1049.

[77] O. Tshekiso, L. Chacha, A. Gueye, and H. Hibshi, "Scaling cybersecurity education in africa: Insights from a capacity-building initiative," in *Proceedings of the ACM Global on Computing Education Conference 2025 Vol 1*, ser. CompEd 2025. ACM, Oct. 2025, pp. 261–267.

[78] W. Aspray, *Participation in Computing: The National Science Foundation's Expansionary Programs*. Springer International Publishing, 2016.

[79] ——, *Women and Underrepresented Minorities in Computing*, ser. History of computing. Switzerland: Springer, 2016, includes bibliographical references and index.

[80] A. Stefik and R. E. Ladner, "Introduction to AccessCS10k and accessible tools for teaching programming," in *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*. ACM, Feb. 2015.

[81] J. L. Glass, S. Sassler, Y. Levitte, and K. M. Michelmore, "What's so special about STEM? a comparison of women's retention in STEM and professional occupations," *Social Forces*, vol. 92, no. 2, pp. 723–756, Aug. 2013.

[82] T. J. Misa, Ed., *Gender Codes: Why Women Are Leaving Computing*. John Wiley & Sons, Jun. 2010.

[83] R. van Veelen, B. Derks, and M. D. Endedijk, "Double Trouble: How Being Outnumbered and Negatively Stereotyped Threatens Career Outcomes of Women in STEM," *Frontiers in Psychology*, vol. 10, 2019.

[84] P. R. Center, "STEM jobs see uneven progress in increasing gender, racialand ethnic diversity," Apr. 2021.

[85] J. D. Skrentny, *Wasted Education: How We Fail Our Graduates in Science, Technology, Engineering, and Math*. Chicago: University of Chicago Press, 2023, description based upon print version of record.

[86] T. Camp, W. R. Adrion, B. Bizot, S. Davidson, M. Hall, S. Hambrusch, E. Walker, and S. Zweben, "Generation CS: The mixed news on diversity and the enrollment surge," *ACM Inroads*, vol. 8, no. 3, pp. 36–42, Jul. 2017.

[87] T. Camp, "'Computing, we have a problem…'," *ACM Inroads*, vol. 3, no. 4, pp. 34–40, Dec. 2012.

[88] U.S. Department of Education, "Digest of education statistics," Institute of Education Sciences, National Center for Education Statistics. [Online]. Available: https://nces.ed.gov/programs/digest/

[89] M. Beldon, W. Dubow, C. Hovey, M. Pollich, and S. Sundar, "NCWIT scorecard: The status of women's participation in computing," Boulder, CO, 2024. [Online]. Available: https://ncwit.org/resource/scorecard/

[90] J. Han and D. Tomaskovic-Devey, "Is tech sector diversity improving?" Center for Employment Equity, University of Massachusetts Amherst, techreport, 2022.

[91] M. T. Neely, P. Sheehan, and C. L. Williams, "Social inequality in high tech: How gender, race, and ethnicity structure the world's most powerful industry," *Annual Review of Sociology*, vol. 49, no. 1, pp. 319–338, Jul. 2023.

[92] F. Dobbin and A. Kalev, *Getting to Diversity: What Works and What Doesn't*. Belknap Press: An Imprint of Harvard University Press.

[93] A. H. Wingfield, "After DEI: A different future for race, work, and policy," *American Sociological Review*, vol. 91, no. 1, pp. 1–18, Dec. 2025.

[94] E. R. Carter, I. N. Onyeador, and N. A. J. Lewis, "Developing & delivering effective anti-bias training: Challenges & recommendations," *Behavioral Science & Policy*, vol. 6, no. 1, pp. 57–70, 2020.

[95] D. Tomaskovic-Devey and D. R. Avent-Holt, *Relational Inequality: An Organizational Approach*. Oxford University Press, 2019.

[96] A. Kalev, F. Dobbin, and E. Kelly, "Best practices or best guesses? assessing the efficacy of corporate affirmative action and diversity policies," *American Sociological Review*, vol. 71, no. 4, pp. 589–617, Aug. 2006.

[97] L. B. Edelman, *Working Law: Courts, Corporations, and Symbolic Civil Rights*, ser. Chicago Series in Law and Society. Chicago: University of Chicago Press, 2016, description based on publisher supplied metadata and other sources.

[98] D. Tomaskovic-Devey, *Gender & Racial Inequality at Work: The Sources & Consequences of Job Segregation*, ser. Cornell studies in industrial and labor relations. Ithaca, NY: ILR Press, 1993, no. 27, literaturverz. S. [196] - 205.

[99] D. Thakkar, "The unexpected entry and exodus of women in computing and HCI in india," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*. ACM Press, 2018.

[100] V. Galpin, "Women in computing around the world," *ACM SIGCSE Bulletin*, vol. 34, no. 2, pp. 94–100, Jun. 2002.

[101] Y. Chen and A. J. Lu, "Immigrant tech workers for, in, and as crisis: The pursuit of global computing leadership," in *Proceedings of the sixth decennial Aarhus conference: Computing X Crisis*, ser. AAR 2025. ACM, Aug. 2025, pp. 42–55.

[102] S. B. Amrute, *Encoding Race, Encoding Class: Indian IT Workers in Berlin*. Durham: Duke University Press, 2016, includes bibliographical references (pages 203-251) and index.

[103] T. Raja. "Gangbang Interviews" and "Bikini Shots": Silicon Valley's Brogrammer Problem. [Online]. Available: https://www.motherjones.com/media/2012/04/silicon-valley-brogrammer-culture-sexist-sxsw/

[104] M. Hicks, "De-brogramming the history of computing [think piece]," *IEEE Annals of the History of Computing*, vol. 35, no. 1, pp. 88–88, Jan. 2013.

[105] S. M. Bogart and L. Y. Dhanani, "Strengthening the foundation: Extending beyond moral framing to overcome DEI backlash," *Industrial and Organizational Psychology*, vol. 18, no. 2, pp. 268–271, Jun. 2025.

[106] The White House, "Executive order 14151—ending radical and wasteful government DEI programs and preferencing," Jan. 2025. [Online]. Available: https://www.federalregister.gov/documents/2025/01/29/2025-01953/ending-radical-and-wasteful-government-dei-programs-and-preferencing

[107] B. Y. Lee, "These 197 Terms May Trigger Reviews Of Your NIH, NSF Grant Proposals," Mar. 2025. [Online]. Available: https://www.forbes.com/sites/brucelee/2025/03/15/these-197-terms-may-trigger-reviews-of-your-nih-nsf-grant-proposals/

[108] B. Mosley, "NSF Cancels DEI and Disinfo/Misinfo Awards Citing Shift in Priorities," Apr. 2025. [Online]. Available: https://cra.org/govaffairs/blog/2025/04/nsf-cancels-awards-april-2025/

[109] J. Schwabish and J. Axelrod, "NSF Has Canceled More Than 1,500 Grants. Nearly 90 Percent Were Related to DEI." Jul. 2025. [Online]. Available: https://www.urban.org/urban-wire/nsf-has-canceled-more-1500-grants-nearly-90-percent-were-related-dei

[110] b. hooks, *Feminism Is for Everybody: Passionate Politics*. South End Press, 2000.

[111] S. J. Khader, *Decolonizing Universalism: A Transnational Feminist Ethic*. Oxford University Press, 2019.

[112] D. Allen, *Difference without Domination*, R. Somanathan, Ed. Chicago: University of Chicago Press, 2020, description based on publisher supplied metadata and other sources.

[113] A. Kalev and F. Dobbin, "The Surprising Benefits of Work/Life Support," *Harvard Business Review*, Sep. 2022. [Online]. Available: https://hbr.org/2022/09/the-surprising-benefits-of-work-life-support

[114] K. R. Fulton, S. Katcher, K. Song, M. Chetty, M. L. Mazurek, C. Messdaghi, and D. Votipka, "Vulnerability discovery for all: Experiences of marginalization in vulnerability discovery," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, May 2023, pp. 1997–2014.

[115] A. Yardim, S. A. Horstmann, R. Serafini, J. G. Speckels, and A. Naiakshina, "Women security experts are not the enemy: A qualitative study on gender-related communication challenges," in *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, ser. CHI '25. ACM, Apr. 2025, pp. 1–27.

[116] B. M. Ferdman, "Paradoxes of inclusion: Understanding and managing the tensions of diversity and multiculturalism," *The Journal of Applied Behavioral Science*, vol. 53, no. 2, pp. 235–263, Apr. 2017.

[117] ——, "The practice of inclusion in diverse organizations," in *Diversity at Work: The Practice of Inclusion*, B. M. Ferdman and B. R. Deane, Eds. Wiley, Nov. 2013, pp. 3–54.

[118] C. Fine, V. Sojo, and H. Lawford-Smith, "Why does workplace gender diversity matter? justice, organizational benefits, and policy," *Social Issues and Policy Review*, vol. 14, no. 1, pp. 36–72, Dec. 2019.

[119] R. Rosenzweig, "Wizards, bureaucrats, warriors, and hackers: Writing the history of the internet," *The American Historical Review*, vol. 103, no. 5, pp. 1530–1552, Dec. 1998.

[120] J. S. Light, "When computers were women," *Technology and Culture*, vol. 40, no. 3, pp. 455–483, 1999.

[121] D. Grier, *When Computers Were Human*. Princeton: Princeton University Press, 2005.

[122] S. Parekh, "Feminism, structural injustice, and responsibility," 2017.

[123] N. Ensmenger, *The Computer Boys Take Over: Computers, Programmers, and the Politics of Technical Expertise*. Cambridge, Mass: The MIT Press, 2010.

[124] J. Abbate, *Recoding Gender: Women's Changing Participation in Computing*. Cambridge, Mass: The MIT Press, 2012.

[125] N. Ensmenger, *Making Programming Masculine*. John Wiley & Sons, Jun. 2010, ch. 6.

[126] N. L. Ensmenger, "The 'question of professionalism' in the computer fields," *IEEE Annals of the History of Computing*, vol. 23, no. 4, pp. 56–74, 2001.

[127] N. Ensmenger and W. Aspray, *Software As Labor Process*. Springer Berlin Heidelberg, 2002, pp. 139–165.

[128] E. Oost, *Making the Computer Masculine*. Springer US, 2000, pp. 9–16.

[129] (2022) Diversity, equity, and inclusion: Anyone, from any background, should feel encouraged to participate and contribute to ACM. [Online]. Available: https://www.acm.org/diversity-inclusion

[130] K. Shorter-Gooden, "Creating diverse and inclusive colleges and universities," in *Diversity at Work: The Practice of Inclusion*, B. M. Ferdman and B. R. Deane, Eds. Wiley, Nov. 2013, ch. 16.

[131] "Supplemental materials," https://osf.io/wkeqs/overview?view_only=a1eb2ad9ce454be6887cc7ac2d28e09e.

[132] S. J. Tracy, *Qualitative Research Methods*, second edition ed. Hoboken, NJ: Wiley Blackwell, 2020, includes bibliographical references and index.

[133] K. Charmaz, *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*. SagePublication Ltd, London, 2006. [Online]. Available: http://www.amazon.com/Constructing-Grounded-Theory-Qualitative-Introducing/dp/0761973532

[134] J. Corbin, A. Strauss, and A. L. Strauss, *Basics of qualitative research*. Sage, 2014.

[135] N. McDonald, S. Schoenebeck, and A. Forte, "Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice," *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, pp. 1–23, Nov. 2019. [Online]. Available: https://dl.acm.org/doi/10.1145/3359174

[136] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa

[137] S. Bardzell and J. Bardzell, "Towards a feminist HCI methodology: Social science, feminism, and HCI," in *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI '11)*, 2011, pp. 675–684.

[138] A. G. D. Holmes, "Researcher positionality–a consideration of its influence and place in qualitative research–a new researcher guide." *Shanlax International Journal of Education*, vol. 8, no. 4, pp. 1–10, 2020.

[139] A. Schlesinger, W. K. Edwards, and R. E. Grinter, "Intersectional HCI: Engaging identity through gender, race, and class," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. New York, New York, USA: ACM Press, 2017, pp. 5412–5427.

[140] V. Braun and V. Clarke, "Toward good practice in thematic analysis: Avoiding common problems and be(com)ing a knowing researcher," *International Journal of Transgender Health*, vol. 24, no. 1, pp. 1–6, Oct. 2022. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC9879167/

[141] J. Henrich, S. J. Heine, and A. Norenzayan, "The weirdest people in the world?" *Behavioral and Brain Sciences*, vol. 33, no. 2–3, p. 61–83, 2010.

[142] A. Kofman, "Can #MeToo Change the Toxic Culture of Sexism and Harassment at Cybersecurity Conferences?" Jun. 2018. [Online]. Available: https://theintercept.com/2018/06/19/metoo-cybersecurity-infosec-sexual-harassment/

[143] J. Leggio, "Beyond the Buzz: Rethinking Alcohol as a Cybersecurity Bonding Ritual," Apr. 2024. [Online]. Available: https://www.securityweek.com/beyond-the-buzz-rethinking-alcohol-as-a-cybersecurity-bonding-ritual/

[144] E. J. Castilla and S. Benard, "The paradox of meritocracy in organizations," *Administrative science quarterly*, vol. 55, no. 4, pp. 543–676, 2010.

[145] E. Berrey, R. L. Nelson, and L. B. Nielsen, *Rights on Trial*. Chicago: University of Chicago Press, 2017. [Online]. Available: https://doi.org/10.7208/9780226466996

[146] R. Sommer, "Small group ecology." *Psychological bulletin*, vol. 67, no. 2, pp. 145–152, 1967.

[147] T. R. Collective, "Safe space: Towards a reconceptualization," *Antipode*, vol. 46, no. 5, pp. 1346–1365, 2014. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/anti.12089

[148] J. Oksala, "Feminism and power," 2017.

[149] A. Allen, "Feminist Perspectives on Power," in *The Stanford Encyclopedia of Philosophy*, fall 2022 ed., E. N. Zalta and U. Nodelman, Eds. Metaphysics Research Lab, Stanford University, 2022. [Online]. Available: https://plato.stanford.edu/archives/fall2022/entries/feminist-power/

[150] I. M. Young, *Justice and the Politics of Difference*. Princeton, NJ: Princeton University Press, 1990.

[151] S. Harding, *Objectivity and Diversity: Another Logic of Scientific Research*. University of Chicago Press, May 2015.

[152] S. J. Khader, "Neoliberalism, global justice, and transnational feminisms," 2017.

[153] D. A. Thomas, "Mentoring and irrationality: The role of racial taboos," *Human Resource Management*, vol. 28, no. 2, p. 279, 1989.

[154] K. Dickinson, T. Jankot, and H. Gracon, "Sun mentoring:1996–2009, technical report smli tr-2009-185," Tech. Rep., 2009.

[155] I. Padavic, R. J. Ely, and E. M. Reid, "Explaining the persistence of gender inequality: The work–family narrative as a social defense against the 24/7 work culture," *Administrative Science Quarterly*, vol. 65, no. 1, pp. 61–111, 2019.

[156] D. Schneider and K. Harknett, "It's about time: How work schedule instability matters for workers, families, and racial inequality," Tech. Rep., 2019.

Gender	**Count**
Man	13
Woman	5
Self-Described	0
Age (Years)	**Count**
20-24	4
25-29	2
30-34	0
35-39	5
40-44	2
45-49	2
50-54	0
55-59	1
60+	0

Race/Ethnicity	**Count**
Asian	5
White	12
Declined	1
Education	**Count**
High school	3
Some college	1
Bachelor's degree	4
Graduate degree	10

TABLE 2: Participant Demographics

Appendix A. Ethical Considerations

Our study was reviewed and approved by our institution's ethics review board. We obtained informed consent from our participants prior to beginning each interview, and we reminded participants of key consent information at the start of each interview, including that we would record audio and extract a transcript with Zoom's built-in transcription service. We assured participants they could skip any question they did not feel comfortable answering.

Our recruitment messages and consent form indicated participation would not be compensated. We chose not to compensate participants since in our prior interactions with this community, participants had declined compensation. Our participants were generally experts volunteering their time to organize cybersecurity communities, and so any compensation we could offer them would likely not be commensurate with their salaries, and we expected them to be more motivated by giving back to the community.

We considered the most harmful outcome of our research would be revealing some information that could be used to infer the identity of one of our participants. As such, we have taken great caution to avoid reporting any information that could be used alone or in connection with other information to identify any participant. We note that multiple US-based participants expressed some concern that discussing topics that could be ambiguously interpreted as Diversity, Equity, and Inclusion could negatively impact their professional future. At the same time, we believe our analysis of welcoming practices has the potential to benefit the cybersecurity community by categorizing what best supports the mission of creating more welcoming environments. Thus, we believe the benefits of publishing this research outweigh any potential harm.

Appendix B.
Meta-Review

The following meta-review was prepared by the program committee for the 2027 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

B.1. Summary

This paper presents a qualitative study that investigates the practices event organizers have adopted to ensure a welcoming environment for newcomers into the cybersecurity community. The paper identifies several different approaches to welcoming as well as some of the challenges faced by organizers.

B.2. Scientific Contributions

- Independent Confirmation of Important Results with Limited Prior Research
- Addresses a Long-Known Issue
- Provides a Valuable Step Forward in an Established Field
- Establishes a New Research Direction

B.3. Reasons for Acceptance

1) This paper provides a study that confirms prior results in the computer science community more broadly regarding how welcoming the culture is to newcomers.
2) This paper addresses the long-known issue of how new attendees can decide against continuing in cybersecurity by providing a series of recommendations based on the experiences of event organizers.
3) This paper provides a valuable step forward by providing recommendations that can be adopted by other event organizers to help make cybersecurity community events and organizations more welcoming.
4) This paper establishes a new research direction by looking specifically at cybersecurity communities and interviewing event organizers, rather than focusing on the experience of attendees (or the computer science community more broadly).