

Project Summary - ITWF Research: Women and Cyber Security: Gendered Tasks and (In)equitable Outcomes. H.R.Rao, Management Systems (PI), S. Bagchi-Sen, Geography (Co-PI), S. Upadhyaya, Computer Science and Eng. (Co-PI), SUNY Buffalo, NY 14260

The purpose of this study is to examine women's entry, retention and advancement in cyber security. Cyber security has been identified by the Department of Homeland Security as one of the critical areas of the national strategy for homeland security. The national strategy to secure cyberspace articulates a national cyber security program and one of the missions is to address the shortfalls in the numbers of trained and certified cyber security personnel.

([http://www.dhs.gov/interweb/assetlibrary/National Cyberspace Strategy.pdf](http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf) February 2003).

Several studies have documented gender inequities in Information Technology (IT) or why this field does not attract women. Our study is informed by this literature which accepts the theoretical premise that women's career outcomes in IT are socially structured. Within this theoretical context, the proposed research selects a hitherto unexplored research arena, cyber security, to get a deeper understanding of career trajectories and to learn how women's experiences can be utilized to formulate new strategies for women's advancement in this arena. A related goal is to understand how institutional intervention promotes gender equity. Three additional objectives of this research are: to explore the existence of differential technical specializations such as mathematical versus societal, legal aspects of security along gender lines, the implication of such differences on career advancement, and to understand why and when such differentiation takes place. We hope that the empirical analysis can be used to ultimately upgrade the competitive position of women in cyber security.

Three broad categories of workforce in cyber security will be studied by our multidisciplinary team through surveys and in-person interviews: (1) Undergrad / graduate men and women who are recipients of the scholarships from the Department of Defense (DoD) Information Assurance (IA) Scholarship Program (IASP) in 50 Centers of Excellence in IA across the nation. Three groups will be used: a cohort of recent graduates, second year students and new entrants. (2) Cyber security professionals with certification from the (ISC)² Institute and who are currently in various cyber security positions across industry sectors. (ISC)² is the non-profit international leader, dedicated to training, and certifying information security professionals. (3) A select group of women who are chief information/security officers in U.S. companies.

The **intellectual merit** of the proposed study is that it addresses gendering of tasks within cyber security, the role of institutional intervention, and implications for career advancement. Our approach differs significantly from previous and ongoing IT studies in that (a) we focus on three different types of workforce, (b) we focus on cyber security - an area of national security - to examine career trajectories of women vis-à-vis men and (c) we examine if there is a gendered division of labor affecting women's labor market outcomes in cyber security, a sub-field of IT. In sum, this study will provide a clear understanding of how female-male (in) equities enter the education and work environment in this relatively new arena. It is possible that factors working against women in IT may be magnified in the cyber security community. It is also possible that factors working against women in IT may be weaker in the cyber security community.

The **broader significance** of the study flows from the fact that our findings could be used to support curriculum design in schools and universities to promote enhanced participation of women in cyber security. Ultimately, the wider societal importance is that a deeper understanding of career trajectories is needed to facilitate women's role as an agent of technological change rather than a passive recipient of new technologies. Our study will help disseminate this knowledge through training grads (including two doctoral students) and undergrads especially women and minority, research publications, web sites, workshops with local schools and teaching colleges, and direct feedback to the community of participants. As part of outreach activities we are cooperating with a sister teaching institution, Buffalo State College, an inner city college, for pilot cyber security workshops targeted at girls in middle and high schools.