□□ **European Commission**

Policy Brief

Addressing Gender Attitude Gaps in Cybersecurity Career Intentions*

Prepared for:
European Commission

Prepared by:
Professor Vladlena Benson

Date: 2025

Context

Recent findings from the She@Cyber project reveal a decisive insight into gender disparities in cybersecurity: women's attitudes toward the field—not skill level, confidence, or capability—are the primary factor influencing their lower intentions to pursue cybersecurity education and careers. This highlights a critical opportunity for policy interventions aimed at reshaping perceptions, increasing visibility, and improving early exposure to cybersecurity across Europe.

Key Findings

The She@Cyber research demonstrates that men consistently display stronger intentions than women to pursue cybersecurity education, reflecting persistent structural and cultural challenges within the STEM and digital sectors. This gap appears despite ongoing efforts to enhance gender diversity, underscoring that existing initiatives do not sufficiently address the underlying factors shaping women's career choices.

A striking finding is that women's self-efficacy—their confidence in their ability to succeed—is comparable to that of men. This challenges assumptions that women are deterred by a lack of confidence or technical ability. Instead, the research shows that attitudes toward cybersecurity play a far more significant role. Many women perceive cybersecurity as highly technical, isolating, or misaligned with their interests, often due to early stereotypes, limited exposure, and the absence of visible female professionals within the sector. These perceptions shape women's beliefs about whether cybersecurity is a suitable, rewarding, and attainable career.

Subjective norms—the social encouragement or expectations individuals perceive—also influence career decisions, but the study shows these norms affect men and women similarly. This reveals that social support alone is insufficient to counteract the attitudinal barriers women face. Additionally, concerns about work–life balance and the perceived intensity of cybersecurity roles contribute to women's hesitation to pursue careers in the field. These perceptions, even when they do not fully reflect workplace realities, significantly reduce women's interest in entering or advancing within cybersecurity.

Together, these findings highlight that addressing attitudes, visibility, and cultural perceptions is critical for increasing women's participation in cybersecurity. Interventions targeting these areas are likely to have an immediate and measurable impact.

Policy Recommendations

1. Rebrand Cybersecurity as a Diverse, Creative, High-Impact Field

- EU-level communication campaigns highlighting women in cyber emergency response, policy, forensics, AI security, etc.
- Embed cybersecurity into school curricula as a creative problem-solving field.

2. Ensure Early Exposure for Girls (Ages 10–16)

- Support EU-wide "Girls in Cyber" bootcamps using She@Cyber training resources.
- Promote female-led cybersecurity hackathons and innovation challenges.

3. Integrate Attitude-Shaping Interventions into Education

- Use real-world case studies demonstrating cybersecurity's societal benefit.
- Highlight accessible career pathways beyond advanced technical roles.

4. Professionalise Career Guidance Across Member States

- Establish an EU Digital Career Guidance Standard.
- Train counsellors to recognise and challenge gendered assumptions.

5. Improve Representation in Teaching & Training

- Recruit and train more female cyber educators and trainers through EU-funded programmes.
- Provide incentives for women to become VET trainers in digital security.

6. Support Family-Sensitive Employment Practices

- Encourage cybersecurity employers to adopt flexible scheduling, hybrid models, and predictable hours.
- Include work–life balance indicators in EU cybersecurity workforce initiatives.

Expected Outcomes

Addressing attitudinal barriers will increase women's interest in cybersecurity education, expand the pool of applicants for cybersecurity roles, and ultimately strengthen the innovation capacity and resilience of Europe's cybersecurity workforce.