Inclusivity, diversity, and gender equality in cybersecurity

The rapid development of digital and communication technologies has revolutionised humanity; however, cyber attacks pose a constant threat that transcends national boundaries. As such, collaborative international approaches to cybersecurity are needed. Cybersecurity has traditionally been a male-dominated field. However, at Cardiff Metropolitan University in the UK, Dr Liqaa Nawaf and her colleagues have established a new, British Council-funded initiative to promote improved gender equality in this field. The project, a collaboration between two world-leading higher education (HE) institutes in the UK and Saudi Arabia – CMU and King Abdulaziz University (KAU) – is an active member of the Women in Cyber Wales Cluster. Now, based on her experiences as a woman working in this field, Nawaf and her colleagues have established an ambitious British Council-funded project to support and increase the role of women in cybersecurity.

PARTNERSHIP FOR EDUCATION AND RESEARCH PROGRAMME

Given the ever-changing threat landscape of cybersecurity, updated knowledge and skills training is critical for those working within the field. The Partnership for Education and Research (PER) Programme for Women in Cyber is a year-long project that started in 2022. It aims to ‘enhance the knowledge, skills training, and research and innovation opportunities of women in cybersecurity disciplines.’

The project is building bridges between two world-leading higher education (HE) institutes in the UK and Saudi Arabia – CMU and King Abdulaziz University (KAU) – intending to facilitate training courses, research collaborations, and ecosystems for women in cyber, including those in the academic, industry, and regulatory sectors. In this way, PER aims to address the inequalities faced by women accessing cybersecurity career paths.

EIGHT BENEFICIARIES

With its goal of improved gender equality, Nawaf envisions eight main groups of beneficiaries: (1) female post-graduate (MSc and PhD) students at participating institutions; (2) girls/women with an interest in enrolling in Cybersecurity degree programmes; (3) the Cybersecurity, Information Networks Centre (CINC) of CMU; (4) the two participating institutes themselves, who will benefit economically and from a new influx of talent; (5) members of related cybersecurity and education committees; (6) the UK and Welsh governments, who will also reap economic benefits and secure new incoming talent to the HE sector; (7) female members of WiCys, the Cyber Wales ecosystem, and other related university societies; (8) and finally, all staff involved in the initiative, for whom participation will offer pathways for career development and progression.

FIVE MAIN OBJECTIVES

The PER project has five main objectives. First, it aims to promote and design a new curriculum – based on sharing best practices – to attract more women into cybersecurity disciplines. Second, it seeks to improve knowledge, skills, and training in cybersecurity among women working in STEM (science, technology, engineering, and mathematics) industries in Saudi Arabia and the UK. Third, it aims to create a strong collaborative partnership between CMU and KAU, facilitating world-leading research and impactful academic collaborations, with a focus on women in cybersecurity disciplines. Fourth, the project will establish a framework for a joint Saudi British Arabian PhD programme supported by a comprehensive mentorship agenda and senior staff with extensive experience in academic success (eg, securing funding). Finally, the PER leaders hope to establish a robust Women in Cyber ecosystem between CMU and KAU.

THREE PHASES

Meeting the aims of the PER initiative involves a three-phase approach.

Phase 1 involves the sharing of knowledge and best practices between CMU and KAU. For example, from one perspective, enrolment of women into cyber disciplines is currently higher at KAU than at CMU. It is hoped that KAU partners will effectively share knowledge.
Phase 3 of PER, the final stage, will establish joint intellectual property rights. Together, these research activities will establish a joint PhD programme with funding opportunities open to the framework and networks for research. Firstly, this includes establishing a joint-CTF events open to students from both CMU and KAU, and one competition event.

Phase 2 of PER is focused on research. Secondly, PER will establish a joint PhD programme with research supervision of enrolled students from academics at both CMU and KAU. Together, these research activities will create new knowledge, economically benefit both the host institutions and their host countries, and result in the establishment of joint intellectual property rights.

Phase 3 of PER, the final stage, will stretch beyond the initial one-year project duration – and will focus on strengthening the strategic links between CMU and KAU. Essentially, this will be a phase of capacity building, with the continuation and further development of the initiatives launched in phases 1 and 2. In particular, research collaborations will continue to deepen, with hoped-for success in securing new funding. In addition, Phase 3 will see the establishment of a Women in Cybersecurity ecosystem between the member organisations and their host countries; this ecosystem will also welcome participants from other HE intuitions, industry, and regulatory bodies in both Saudi Arabia and the UK.

**PER: OUTCOMES**

The project has already achieved many outcomes, including implementation of a joint Saudi-UK PhD programme for cybersecurity; sustained collaborative research between CMU and KAU including development of joint research grant applications; and the establishment of Women in Cyber Ecosystem between the two countries. As Nawaf explains, "Through a partnership approach, we have already realised many outcomes from this project. We have shown real impact in making a difference to building the confidence of females studying and working in cybersecurity. In turn, cybersecurity will become more diverse which will be of significant value to the Welsh, UK, and SA economies."

**PER: FUTURE GOALS**

In addition to achieving the aims and goals of the three phases, the PER project aims to disseminate knowledge further via conference presentations, peer-reviewed journal articles, and chapters in relevant book volumes. Each of these media will offer a platform to share the lessons learned during the project and present research arising from the new collaborations. More widely, it is hoped that the PER project will get coverage on national and international media platforms, including across traditional news outlets and social media. PER could enhance the knowledge, skills training, research and innovation opportunities for women in cybersecurity. Therefore, should the goals laid out here, PER will successfully increase the inclusivity and diversity of cybersecurity disciplines at the partner institutions – and, more broadly, enhance the opportunities open to women in technology. Given the ever-changing threat landscape of cybersecurity, updated knowledge and skills training is critical for those working within the field.