OPEN ACCESS Freely available online

Journal of Defense Management

Editorial

Editorial on Cyber Security Education

Sanike Swapna*

Department of Political Sciences, Osmania University, Hyderabad, Telangana, India

EDITORIAL

Many recent reports of cyber security attacks show that a wide spectrum of harmful conduct is common, and that cyber threats are becoming more sophisticated. These risks have a wide range of consequences for governments, organisations, and individuals all around the world. Frameworks aimed at addressing the cyber security issue Focus on the need to strengthen cyber security capabilities at the national level.

Building labour capacity necessitates the creation of strategic and operational frameworks, which are frequently lacking in poor countries. As a result, knowing the limits that those countries confront is a critical first step in determining how to develop cyber security. This study analyses the obstacles faced by Ecuador's higher educational system in cyber security education and then evaluates potential for development through a qualitative thematic analysis of interviews with leaders in higher education.

Many areas of cyber security education have been addressed as part of national capacity building programmes, workforce development, and studies focused on education. The US Department of Homeland Security, the US National Institute of Standards and Technology, and the US National Institute of Standards and Technology have comprehensively documented issues related to both the scarcity of cyber security professionals and strategies for improvement in developed economies.

The US Department of Homeland Security The UK Government Communications Headquarters, the UK Government Communications the United Nations, the European Union, and "think tanks" like the International Crisis Group The RAND Corporation, Booz-Allen Hamilton, and the SANS Institute are all part of the RAND Corporation. Among other things however, literature that focuses on in undeveloped countries, such difficulties are minor. Education is a critical component of the United States' national cyber security preparation, and legislation and methods to enhance cyber security education and a workforce have been enacted.

The National Initiative for Cyber security Education (NICE) was established to strengthen the United States' long-term cyber security posture. Awareness, formal education, professional training, and workforce structure are all addressed by NICE. NIST developed the National Cyber security Workforce Framework to support this programme, which provides a common language (lexicon and taxonomy) for academics to utilise. This contains seven cyber security areas of provision, job responsibilities, and related skills, which are being used to construct academic programmes at various US colleges. These programmes are also backed up by a qualified workforce (i.e., people with extensive cyber security experience) that may be found in the sector by US educational institutions. In fact, despite high sector compensation, educational institutions participating in RAND's poll (2014) find little difficulty in hiring individuals from the cyber security market. Despite this, the United States continues to struggle to establish a competent cyber security workforce. According to a research conducted by the SEI, there are issues about the appropriateness of cyber security measures used by employees in the workplace, as well as workforce readiness to effectively defend IT infrastructure.

Correspondence to: Sanike Swapna, Department of Political Science, Osmania University, Hyderabad, Telangana, India, Tel: +92-323 - 9991029; E-mail: sanike.swapna709@gmail.com

Received: July 15, 2021; **Accepted:** July 20, 2021; **Published:** July 25, 2021

Citation: Swapna S (2021) Editorial on Cyber Security Education. J Defense Manag, Vol.11 No.213