GUEST EDITORIAL PREFACE

Special Issue on Cyber Defence in Southern African Region

Joey Jansen van Vuuren, Council for Scientific and Industrial Research, Pretoria, South Africa

Due to the exponential growth in broadband access, the use of wireless technologies and infrastructure, high levels of computer illiteracy, and ineffective or insufficient legislation to deal with cyberattacks and threats contribute to African countries being very vulnerable to cybercrimes. In 2011, South Africa was already rated as the third highest country in the world for cyberattacks (cybercrime and other attacks). This situation has not really changed much during past four years. There is a focus by governments to develop strategies and frameworks to secure cyber space in order to reduce these threats and defend against cyberwarfare.

Jacquire and Von Solms discuss collaboration between African countries to use a regional security plan that can act as a shield against attacks. Ethics plays a major role in all these frameworks and policies and careful consideration must be given to this aspect in cybersecurity plans. Burmeister et al. discuss the ethical elements of the South African Cybersecurity policy as well as the aspects of attribution. Veerasamy and Grobler use scenarios to set up a classification system to identify if an attack can be classified as cyber terrorism. Pillay focuses on Web 2.0 technologies and the impact of the adoption of these technologies on civil societies' roles, structure, and orientation.

Joey Jansen van Vuuren
Guest Editor
IJCWT