Editorial Preface

Brett van Niekerk, University of KwaZulu-Natal, Durban, South Africa
Graeme Pye, Deakin University, Deakin, Australia

It is with great pleasure that we would like to present this second issue of the International Journal of Cyber Warfare and Terrorism (IJCWT) for 2019. This publication contains four articles submitted to the journal for consideration.

The IJCWT publishes original innovative findings on ethical, political, legal, and social issues relating to security and cybernetic wars. This journal focuses on cyber warfare, security and terrorism using examples from around the world. IJCWT covers technical aspects, management issues, social issues, and government issues that relate to cyber warfare, security and terrorism.

The mission of the IJCWT is to explore a range of security related topics and generate research debates in relation to cyber warfare, security and terrorism. Targeting researchers, practitioners, academicians, government officials, military professionals and other industry professionals. The IJCWT provides a forum to discuss human, technical, and policy issues in relation to cyber warfare and terrorism.

In this issue of the IJCWT, the following four research articles represent the substantial and expansive research undertaken by the authors' who have submitted their research and discussions to the journal. The articles presented here have undergone a double-blind review process.

The first article, *Dark and Deep Webs - Liberty or Abuse* by Lev Topor, provides a topical discussion on the duality of the Dark Web for protecting those who are oppressed but are advocating for human rights, versus the use for other socially nefarious means. An important question of accountability for the Dark Web is also raised.

The second article, titled *Social Media Networking and Tactical Intelligence Collection in the Middle East*, is authored by Karen Howells. The authors discuss the use of social media and associated technologies as an open source intelligence tool with the specific focus on cases from the Middle East. Current and technological developments, such as the use of artificial intelligence, are considered. A combination of social bots and data mining is proposed as the next stage for open source intelligence collection on social media.

The third article, *Role of Cyber Law and Mitigation Strategies in perspective of Pakistan to cope Cyber Threats* by Jawad Hussain Awan, Shahzad Memon and Fateh Muhammad Burfat, provides a review of the cybersecurity landscape in Pakistan and a critical analysis of the Pakistani cyber law as compared to other international cyber laws. Possible shortcomings are identified and recommendations made to improve the cyber law in Pakistan.

The fourth article, *Provably Secure Private Set Intersection with Constant Communication Complexity*, is authored by Sumit Kumar Debnath. The author proposes a private set intersection protocol. The security of the proposed protocol is analysed by a mathematical proof. He concludes that the proposed scheme provides constant communication complexity with a linear computational cost.

Brett van Niekerk
Graeme Pye
Editors-in-Chief
IJCWT