Editorial Preface

Brett van Niekerk, University of KwaZulu-Natal, Westville, South Africa
Graeme Pye, Deakin University, Geelong, 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 2018. 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 and varied research articles represent the substantial and expansive research undertaken by the authors' who have submitted their research and discussions to the journal. The first three manuscripts underwent a double-blind peer review process prior to being selected for publication. The fourth manuscript has been expanded from their initial research and discussions as detailed in the *8th International Conference on Internet Technologies & Society* (ITS 2017).

The first article, *Measuring the World: How the Smartphone Industry Impacts Cyber Deterrence Credibility* by Dirk Westhoff and Maximilian Zeiser, explores how swarm-mapping (crowd sourcing) is used to obtain geo-location information on wireless access points and mobile telecommunication systems' base stations. The authors then propose how this potentially influences cyber deterrence strategies of states. The manuscripts concludes that worldwide location harvesting with swarm mapping can be considered as a powerful tool for deterrence-by-retaliation.

The second article, *On Experience of Social Networks Exploration for Comparative Analysis of Narratives of Foreign Members of Armed Groups: IS and L/DPR in Syria and Ukraine in 2015-2016* by Yuriy V. Kostyuchenko, Maxim Yuschenko, and Igor Artemenko, investigates the use of probabilistic and stochastic methods of analysis and classification of data from social network to provide a comparison of narratives of foreign members of armed groups in Iraq and Ukraine. The manuscript motivates that narrative analysis is an important technique for security monitoring and control. The authors conclude that there is a similarity between the internal logic of the two conflicts, implying a common driving force of terrorism on a global scale.

The third article, *Punching Above Their Digital Weight: Why Iran is Developing Cyberwarfare Capabilities Far Beyond Expectations* by Ralph Martins, explores the ideological drivers and historical events related to the growth of Iranian cyber power. The manuscript concludes that through cyber-space capabilities, Iran has found a mechanism to for pursuing its national security goals and respond to international pressures against the state.

Lastly, the fourth article, *Framework for Military Applications of Social Media* by Namosha Veerasamy and William Aubrey Labuschagne, examines the implications of social media in the military, as both a beneficial tool and in terms of its malicious uses. The authors propose a framework for the use of social media in military contexts, and conclude that there is a need for education and awareness around the dangers and responsible use of social media.

We acknowledge the contributions made by these researchers and each article provides an interesting example of current research and it is our hope that this collection of research articles will stimulate further research, debate and discussion in the vibrant and topical areas across cybercrime, cybersecurity, cyber terrorism, and cyber warfare.

Brett van Niekerk
Graeme Pye
Editors-in-Chief
IJCWT