

Editorial Preface

Brett van Niekerk, University of KwaZulu-Natal, South Africa

Graeme Pye, Deakin University, Australia

It is with great pleasure that we would like to present this third issue of the International Journal of Cyber Warfare and Terrorism (IJCWT) for 2019. This publication contains three 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 three 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, "Information influence in Hybrid Environment: Reflexive Control as an Analytical Tool for Understanding Warfare in Social Media," is authored by Aki-Mauri Huhtinen, Noora Kotilainen, Saara Särmä, and Mikko Streng. It provides a pertinent discussion on how the concept of 'Reflexive Control' can be applied to the challenges the modern information and media domain present the military, in particular information influence. The authors propose that a shift towards a rhizomatic understanding of warfare, away from the traditional systematic approach by Western military organisations, will provide insights into the contemporary information environment.

The second article, titled "Cyber Terrorism and Self-radicalization. Emergent Phenomena of Onlife Age: An Essay Through the General Systemic Theory" by Primavera Fisogni, employs General System Theory as a theoretical underpinning to investigate the growth of modern terrorism in the intersection of the online and offline worlds. The article concludes that the connection between the online

media inspiring terrorism and the physical act itself has become the key ingredient, rather than ideology.

The third article, “The Impact of Cyber-Physical Warfare on Global Human Security,” is authored by Edward L. Mienie and Bryson R. Payne. The article discusses the evolution of traditional cyber-attacks to cyber-physical attacks, with particular focus on critical infrastructure. The authors provide suggest avenues for the cyber warfare to evolve in the future, and call for political leaders, law enforcement, military, government and critical infrastructure officials to be trained through exercises on dealing with disruptive cyber-attacks.

Brett van Niekerk
Graeme Pye
Editors-in-Chief
IJCWT