Editorial Preface

Special Issue on ICCWS 2016: Part 2

Graeme Pye, School of Information and Business Analytics, Deakin University, Geelong, Australia
Brett van Niekerk, University of KwaZulu-Natal, Durban, South Africa

It is with great pleasure that we would like to present this special issue of the International Journal of Cyber Warfare and Terrorism (IJCWT). This publication is a special issue relating to research articles drawn from the participating researchers at the recent *11th International Conference on Cyber Warfare and Security* (ICCWS) hosted by the Boston University, Boston, USA in March 2016 and the *16th European Conference on Cyber Warfare and Security* (ECCWS) hosted by the University College, Dublin, Ireland in June 2017. A double-blind peer review process was used in determining the conference paper inclusion. This means that the papers we have included in 7(4) are extensions upon previously reviewed papers and therefore do not require further reviews apart from ours as Editors.

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 initial three and varied research articles represent the substantial and expansive research undertaken by the invited authors' who have extended upon their initial research and discussions as detailed in their original ICCWS 2016 conference papers. The fourth article is also an extended research article from the recent ECCWS 2017 conference, with the final contribution of a book review for your consideration to round out and complete this issue.

The first article: *Developing a Military Cyber Security Model for Multi-Domain Battle Mission Resilience and Success* by David Ormond and Benjamin Turnbull discusses an interesting aspect of modern military operations and the increasing integration and reliance upon computing capabilities. Securing such cyber capabilities requires more than an information assurance approach. Therefore, a Military Cyber-Maturity Model is proposed based on business continuity approach utilising cultural change, work practices including analogue and digital and deceptive counterintelligence behaviours to instil resilience, survivability and harden cyber security. With a view that such a cyber-maturity assessment approach is critical to develop and inform future military cyber security doctrine.

The second article: *A Dynamic Cyber Defense Framework* by Jim Q. Chen argues that a dynamic cyber defense framework is needed to supersede current fortress-based and static cyber defense

approaches. To this end, the article outlines the challenges of integrating together a systematic and cohesive framework that integrates across the strategic, operational and tactical aspects of cyber defence. A dynamic cyber defense framework is proposed that utilises contextual analysis and decision-making to provide customised adaptable solutions within the operational and strategic complexity and uncertainty of the cyber security environment.

The third article: *Quantifying Decision Making in the Critical Infrastructure via the Analytic Hierarchy Process (AHP)* by John S. Hurley. Seeks to outline a more consistent and verifiable means to optimise critical infrastructure decision-making within organizations to better manage disruption and attacks on critical infrastructure systems. The pilot study analysis approach applied, extends upon the Analytic Hierarchy Process (AHP) utilising pairwise comparison as a means to inform decision-making and improve critical infrastructure resilience and identify and reduce vulnerabilities. With future research aimed at further refinement, improving predictability and assessment measurable.

The fourth article: *The World is Polluted with Leaked Cyber Data* by Ivan D. Burke and Renier P. van Heerden is an extended paper drawn from the recent ECCWS 2017 conference. The authors outline that the escalating proliferation of data breaches should be regarded as a cyber pollution issue and mapped in a similar manner to physical pollution. To this end the authors outline their experimental approach to modelling data breaches and mapping the network activity of the data breaches as a means of assessing the security of the corporate network assets. This research offers an interesting alternative take on data breaches as cyber pollution and is still in the very early stages of development.

Finally, to close out this issue of the IJCWT. Prof Maximiliano Emanuel Korstanje of the University of Palermo and former past Editor-in-Chief of the IJCWT journal, has kindly contributed an insightful book review of a recently published edited book by Jeremi Suri and Benjamin Valentino entitled *Sustainable Security: Rethinking American National Security Strategy* for your consideration and future reference.

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 cybersecurity, cyber warfare and information security.

Graeme Pye
Brett van Niekerk
Editors-in-Chief
IJCWT