Editorial Preface

Special Issue of CWAR 2018

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

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 *17th Australian Cyber Warfare Conference (CWAR)* hosted by the Deakin University Centre for Cyber Security Research and Innovation and sponsored by the Australian Information Security Association in Melbourne, Victoria, Australia on October 10-11th 2018.

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 and terrorism using examples from around the world. IJCWT covers technical aspects, management issues, social issues, and government issues that relate to cyber warfare 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 and terrorism. Targeting researchers, practitioners, academicians, government officials, military professionals and other industry professionals, 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 five and varied research articles represent the substantial and expansive research undertaken by the invited authors' who have extended their initial research and discussions as elaborated upon in their original conference papers.

The initial article: "Deceiving Autonomous Drones" by William Hutchinson focuses on discussing the concept of deceiving autonomous artificial intelligent (AI) drones and the possible use of deception as a defence or a means of gaining advantage. The article posits that emergent AI technology could expand the capabilities of these devices, raising deep ethical, legal and philosophical concerns in terms of surveillance and kinetic impacts, the use of swarms and the Internet of Things (IoT). Highlighting the need for a broader discussion with relation to human behaviour, responses, potential deception impacts and counter-deception measures as a defence mechanism.

The second article: "Political Cyber Operations: A South Pacific Case Study" by Matthew Warren discusses the prevalence of 'fake news' and the nexus of social media and the impacts on society, citizens, business, and in particular using politics as the basis case study. From a cost-effective perspective, social media enables connections leading to engagement and interaction directly with society and individuals. This article proposes a conceptual information operations assessment model, applied to a political election campaign case study, to validate the model and identify unsubstantiated news postings as a prelude to further research development.

The third article: "Cyber Warfare: An Enquiry into the Applicability of National Law to Cyberspace" by Helaine Leggat and builds further on an initial paper regarding the applicability of a national law for cyberspace, in an international setting. This article proposes that it is time to discuss the prospect of a national law for cyberspace to establish acceptable norms of behaviour in an international setting. The premise being that like the United Nations, private and public entities can

similarly cooperate to establish mutual international norms of acceptable behaviour in cyberspace in terms of cyber warfare and cyber attacks, based on an extensive legal analysis of the Tallinn Manual 2.0.

Our fourth article: "Risks Of Critical Infrastructure Adoption of Cloud Computing by Government" by Mansoor Al-Gharibi, Matthew Warren, and William Yeoh. This research article looks at the adoption of cloud computing within governmental critical infrastructure domains and risks associated with such deployments. The article discusses the risk aspects of various cloud computing deployment models and cloud service types with regard to the mitigation of risks identified, particularly from the cyber warfare perspective. This research is relevant as governments are shifting towards and deploying cloud computing services, thus moving the technology support burden to the cloud provider largely motivated by cost savings and enabling government agencies to focus more on the business model of service delivery, rather than managing the technology risk from within.

Our fifth and final article: "A Study of Cybersecurity Issues in Sri Lanka" by R. T. S. Nagahawatta, Matthew Warren, and William Yeoh evaluates cybersecurity awareness among a cohort of university students in Sri Lanka. This research project identified that there is some functional cybersecurity awareness within this group relating to online incidents based on gender, study field, academic year and province of respondents. However, some existing knowledge gaps do exist relating to social media use, misuse and Sri Lankan legal and regulatory bodies. This article proceeds to discuss capacity building of cybersecurity awareness knowledge in Sri Lanka.

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 information warfare and information security.

Graeme Pye
Brett van Niekerk
Editors-in-Chief
IJCWT