Editorial Preface

Special Issue on the 10th International Conference on Cyber Warfare and Security (ICCWS)

Graeme Pye, Deakin University, Geelong, Australia

Maximiliano Korstanje, University of Palermo, Buenos Aires, Argentina

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 *10th International Conference on Cyber Warfare and Security* (ICCWS) hosted by the University of Venda and the Council for Scientific and Industrial Research at Kruger National Park, South Africa in March 2015.

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 seven 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: *Cyber-security for ICS/SCADA: A South African Perspective* by Barend Pretorius and Brett van Niekerk. Focuses on discussing the cyber security and legislative challenges in relation to securing Industrial Control Systems (ICS) and SCADA systems in South Africa. A high-level governance and security framework is proposed that provides guidance for mitigating potential vulnerabilities, attack methods and threats to ICS and SCADA systems in the South African context. Historical incidents relating to compromised infrastructure systems are discussed and used to inform the structural controls as outlined in the proposed framework.

The second article: *Adaptation of the JDL model for multi sensor national cyber security data fusion* by Ignatius Swart, Barry Irwin and Marthie Grobler outline initial research undertaken highlighting the application of open-source security information against an adaptation of the Joint Directors of Laboratories (JDL) data fusion model. Initially, the authors identify and discuss the elements of data fusion within the South African cyber domain, including the differing characteristics of various data sources, before using them to inform the subsequent adaptation of the JDL model from a national perspective. A cyber case-study is then applied against the adapted JDL model, with findings presented, conclusions drawn and discussed.

The third article: *Deception Detection in Cyber Conflicts: A Use Case for the Cybersecurity Strategy Formation Framework* by Jim Chen focuses on the strategy of deception as applied within the context of cyber conflicts. It is the detection and unveiling of applied deception tactics that lies at the heart of this research, including the challenges of detecting applied deception. The intent here is to deliver a strategic, systematic, holistic and integrative multi-level approach utilising differing contextualised analysis systems as proposed in the Operational-Level Cybersecurity Strategy Formation Framework. Lastly, a case study is developed and discussed as applied to the framework, in order to detect such fabrication and manipulation deceptions within a cyber conflict to inform responsive actions, decision-making and counter strategies.

Our fourth article: *The Next Generation of Scientific-based Risk Metrics: Measuring Cyber Maturity* by Lanier Watkins and John Hurley. Their research looks at the major challenges an organisation should address in order to effectively mitigate against existing and future cyber threats and vulnerabilities. They propose a comprehensive risk-based metrics to assist organisations assess and determine their level of cyber-maturity that focuses of the probability of compromise of given vulnerabilities, employees, insider threats and non-adherence to cyber-based policies. This results in a data-driven, quantifiable Cyber Security Model that enables collective consensus building based on trust and the quantifiable assessment of risk. Particularly, from a comparative organisational aspect and to inform subsequent decisions and mitigation actions.

Our fifth article: *Semantic Technologies and Big Data Analytics for Cyber Defence* by Louise Leenen and Thomas Meyer investigates the ‘big data’ analysis of vast amounts of cybersecurity related data in relation to inform decision-making outcomes. A number of Data Analytics techniques, ontologies, including predictive analytics are discussed and their likelihood to reveal patterns, correlations, trends and other useful insights from large and disparate data sets.

The sixth article: *Using an Ontology for Network Attack Planning* by Renier van Heerden, Peter Chan, Louise Leenen and Jacques Theron presents a Network Attack Planning ontology that provides support in determining counter-measures in response to network attacks. This coupled with the use of semantic technologies, contributes towards the automated reasoning capabilities of ontological-based intelligent processing of information and the unveiling of inferences and relationships. As aspects of warfare move to the cyber domain, the intent here is to extend the capability of the planning ontology to incorporate an operational perspective that serves to enrich information regarding cyber-attack and countermeasure planning.

The seventh and final article: *SCADA Systems Cyber Security for Critical Infrastructures: Case Studies in Multiple Sectors* by Suhaila Ismail, Elena Sitnikova and Jill Slay investigates the resulting financial and economic impacts for cyber-attacks on Supervisory Control and Data Acquisition (SCADA) Systems for critical infrastructures. Nine historical case studies relating to multiple utility sectors are analysed with a view to forming specific organisational SCADA related guidelines for preparing, identifying and mitigating potential future cybersecurity attacks.

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
Maximiliano E. Korstanje
Editors-in-Chief
IJCWT