Editorial Preface

Special Issue on ICCWS 2016:
Part I

Graeme Pye, Deakin University, School of Information and Business Analytics, Geelong, Australia

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 containing peer-reviewed 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.

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 invited authors' who have extended upon their initial research and discussions as detailed in their original ICCWS 2016 conference papers.

The initial article: *Cyberspace: The New Battlefield (An Approach via the Analytics Hierarchy Process)* by John S. Hurley. Discusses the paradigm shift of battlefield conflict from the exclusive conventional warfare domain to the cyberspace domain and that enabling technology has altered the engagement rules, where potential combatants can now emerge from any part of society to instigate attacks via the cyberspace domain. The defense and protection of information assets in cyberspace is discussed through the prisms of organisational culture and trust and the role they play in cyber conflicts across the three societal segments of the public, private and government sectors. The Competing Values Framework and Schein models are examined and a new model (Analytics Hierarchy Process) is proposed to reconcile issues and applied to explore the use of 'active defences' as means to deter cyber-attacks.

The second article: *Formulating the Building Blocks for National Cyberpower* by J.C. Jansen van Vuuren, Louise Leenan, Graeme Plint, Jannie Zaaiman and Jackie Phahlamohlaka outlines the growing risk to national security for all nation states and their capacity to wage cyberwarfare. This research adapts the formula for Perceived Power and proposes a formula to articulate Perceived Cyberpower. In doing so, it highlights the multifaceted attributes and complexity of physical, informational and cognitive variable phenomena as three distinct layers of cyberspace, influencing the perceived capacity of a national cyberpower.

The third article: *Optimization of Operational Large-scale (Cyber) Attacks by a Combinational Approach* by Éric Filiol and Cécilia Gallais focuses on the potential vulnerability of cyber-attacks against critical infrastructures. This research utilises Graph Theory applying the Vertex Cover approach to analyze a model of an electrical power transmission and distribution system to determine and identify the likely critical components within the system. Undertaking a systematic, holistic and integrative multi-level approach utilising this approach may prove a useful approach to those attempting to identify critical infrastructure system weaknesses.

Our fourth and final article: *Advanced Network Data Analytics for Large-scale DDoS Attack Detection* by Konstantinos F. Xylogiannopoulos, Panagiotis Karampelas and Reda Alhajj. Their research investigates to issues of an apparent lack of security standards being applied to the manufacture of Internet–enabled devices within the realm of the Internet of Things and a Distributed Denial of Service (DDoS) context. The research applies a data mining technique to analyse incoming IP (Internet Protocol) traffic as a means to forewarn network administrators of a potential DDoS attack. This results in a data-driven, quantifiable early warning that enables collective actions to be taken to defend networks and identify and block potential DDoS sources, thereby informing organisational and inform subsequent decisions and mitigation actions.

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
Editor-in-Chief
IJCWT