Editorial Preface

Special Issue on the 14th European Conference on Information Warfare and Security 2015 (ECCWS) – Hatfield, UK (Part 2)

Graeme Pye, Deakin University, Geelong, Australia
Maximiliano E. 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 the second of two journal special issues relating to research articles drawn from the participating researchers at the recent *14th European Conference on Information Warfare and Security* (ECCWS) hosted by the University of Hertfordshire in Hatfield, UK in July 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 four and varied research articles represent the substantial and expansive research undertaken by the invited authors who have extended their research and discussions initially elaborated upon in their original conference papers.

The first article: *Situation Understanding for Operational art in Cyber Operations* by Tuija Kuusisto, Rauno Kuusisto and Wolfgang Roehrig present a preliminary theoretical framework designed to assist in identifying emerging phenomena and information requirements to inform planning and decision making. With the focus on wide-ranging operations planning in cyberspace utilising system modelling, social system modelling and human information modeling analysis, a case study is assessed and outcomes discussed accordingly with a view towards increasing situational awareness and creating novel outcomes.

The second article: *Cyber Security Education and Research in the Finland's Universities and Universities of Applied Sciences* by Martti Lehto notes the increasing dependency that governments, businesses and citizens have developed on information and communication technology. As network connectivity has increased, the author highlights the need for highly trained cyber security professionals to develop and implement cyber security solutions and strategies within the public and private sectors. From the European Union and Finish perspective, the author analyses the fundamental of security

research and education at a number of different universities and research institutes, to outline and identify the desirable competences and objectives pertinent to cyber security education.

The third article: *Reconceptualising Cyber Security: Safeguarding Human Rights in the Era of Cyber Surveillance* by Andrew Liaropoulos focuses on shortcomings of the human-centric considerations of cyber security. The author undertakes a wide-ranging discussion related to human rights in cyberspace and provides examples of such violations and the measures employed to perpetrate them, due in-part to dominant state-centric approach taken to cyber security. The author argues that there is need for a shift towards policies that safeguard privacy, freedom of expression and the unjustifiable sharing of personal data.

Finally our fourth article: *SPCTA: An Analytical Framework for Analyzing Cyber Threats by Non-State Actors* by Harry Brown argues that the accessibility and connectedness of the Internet is playing a part in the reputations of nation states and the behaviour of nation-states towards each other based on comparative cyber capability of the state. Within this domain, the emergence of non-state actors can impact state governance, operations and citizens. The author's research looks at non-state actors and proposes a framework for analysing cyber threats from non-state actors. The outcome is a the Social Process Framework for Cyber-Threat Analysis (SPCTA) that may assist practitioners with assessing potential cyber-threats from unsanctioned non-state cyber actors.

Each article provides an interesting example and perspective 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