Editorial Preface

Special Issue on the 14th European Conference on Information Warfare and Security 2015 (ECCWS): Hatfield, UK (Part 1)

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 first 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 initial article: *Cyber Terrorism Taxonomies: Definition, Targets, Patterns, Risk Factors and Mitigation Strategies* by Ali Al Mazari, Ahmed H. Anjariny, Shakeel A. Habib and Emmanuel Nyakwende. Proposes some potential mitigation strategies and countermeasures for a cyber terrorism defined taxonomy drawn from existing military forces, government cyber and physical infrastructures, critical national infrastructure, social and national identity and private industry interpretations based on target, motive, means effect and intent. The outcome is a categorical taxonomy of knowledge to improve awareness and delineation of cyber terrorism through a taxonomy defining boundaries, targets and crimes, including mitigation strategies.

The second article: *Cyber Espionage and Illegitimate Information Retrieval* by Roland Heickerö discusses the potential long-term implications to economic development and threats to national trade, industry of cyber espionage. With these activities increasingly focusing on high technology industries and organisations coupled with enhanced Internet accessibility, it is timely to discuss improving

organisational security with a view to reduce information leakage. While this remains a sensitive issue not readily acknowledged to by organisations. The author examines and discusses a number of incidents of espionage, the methods used, their discovery, possible information losses and subsequent actions taken to resolve and counter these invasive practices.

The third article: *Arts and Branches of Science Significantly Contributing to Cyber and Cyber Security: The West European and the Russian Views* by Margarita Jaitner and Aine MacDermott. Interestingly, this research undertakes a comparative look at cyber security education in academia, from the Western European and Russian perspectives, under the influences of their respective national cyber readiness. While the Western European focus may appear to be based in technology and military related sciences, the Russian approach has a broader domain focus. The authors have identified some notable differences and relevant contributions that other disciplines of academia may contribute and bring to formulating a boarder cyber security education approach in the West.

Our final article: *A White Hat Study of a Nation's Publicly Accessible Critical Digital Infrastructure and a Way Forward* by Timo Kiravuo, Seppo Tiilikainen, Mikko Särelä and Jukka Manner takes a look at the security vulnerabilities within the automated control processes of critical infrastructures. They argue that while industry appreciates the importance of industrial safety, there is not the same level of concern when dealing with information technology security. Through their research findings, the authors argue that there is merit in the continuous monitoring or auditing of a nation's own Internet address space for industrial control process vulnerabilities. However, they also acknowledge that this would require legislative changes, including changes to the roles and responsibilities of associated stakeholders and critical infrastructure protection.

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