Editorial Preface

Brett van Niekerk, University of KwaZulu-Natal, South Africa

Graeme Pye, Deakin University, Australia

It is with great pleasure that we would like to present this second issue of the *International Journal of Cyber Warfare and Terrorism* (IJCWT) for 2020. This publication contains five research articles submitted to the journal for consideration.

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 five research articles represent the substantial and expansive research undertaken by the authors' who have submitted their research and discussions to the journal. The articles presented here have undergone a double-blind review process.

The first article, "Insider Threat Detection Using Supervised Machine Learning Algorithms on an Extremely Imbalanced Dataset," by Naghmeh Sheykhkanloo and Adam Hall, investigates the importance of balancing datasets during pre-processing when using machine learning to aid in insider threat detection. Experimenting with a variety of machine learning algorithms, the impact of balancing on a number of performance metrics was measured. It was concluded that in general balancing did not improve most performance metrics, however the times to build and test the model did improve.

The second article, titled "On the behavior-based risk communication models in crisis management and social risks minimization" is authored by Yuriy V. Kostyuchenko, Viktor Pushkar, Olga Malysheva, and Maxim Yuschenko. The authors contend that there is an anthropological limitation to risk models, being human behaviour. They propose a mathematical model for behaviour-based risk communications, and conclude that dynamic models should be used to propose robust solutions rather than optimal solutions in order to improve social resilience to crises.

The third article, "Predicting and Explaining Cyber Ethics with Ethical Theories," by Winfred Yaokumah, uses a quantitative approach to investigate the relevance of various ethical constructs, Consequence-Based Ethics, Duty-Based Ethics, and Virtue-Based Ethics, on ethical behaviour online. The study indicates that consequence-based ethics is the strongest predictor computer ethics, cyber privacy, academic integrity, whereas duty-based ethics is the strongest predictor of intellectual property rights. The author motivates that ethical theories can therefore be used to educate computer and Internet users about ethical conduct online.

The fourth article, "The Security Aspects of Automotive Over-the-Air Updates," is authored by James Howden, Leandros Maglaras, and Mohamed Amine Ferrag. The article focuses on the software update processes for 'smart' connect vehicles in terms of both the external and internal networks.

The article raises concerns around the ability of the internal vehicle network to support such updates, dated encryption schemes employed, and the possible exposure of vehicles to cyber-attack.

The fifth and final article, by Yadigar Imamverdiyev and Fargana J. Abdullayeva, is titled “Deep Learning in Cybersecurity: Challenges and Approaches.” This article presents a review of published research related to the use of machine learning, and in particular deep learning, techniques for threat detection in cybersecurity. The author also provides a brief overview of industry solutions for cybersecurity incorporating deep learning techniques.

Graeme Pye
Brett Niekerk
Editors-in-Chief
IJCWT