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 first issue of the International Journal of Cyber Warfare and Terrorism (IJCWT) for 2021. IJCWT has now entering is second decade with this issue being the first of volume 11. 2020 was a disruptive year, with the unprecedented events of the COVID-19 pandemic. We were fortunate to be able to continue publishing, where other publications faltered. For this, we would like to thank the authors, reviewers, and editorial staff for their support and enabling the IJCWT to continue to publish all four issues last year and continue strong into this year.

On the cyber front, we saw an increase in disinformation as well as cyber-crime and other online attacks using the pandemic as a lure for phishing and espionage (Montalbano, 2020). In addition, there was a short conflict when Iran was alleged to have targeted the Israeli water systems, and the reported response affected the operations of a major Iranian port (Melman, 2020). Major data breaches continued to occur, with the Experian breach in South Africa being the country's largest, despite the privacy law, the Protection of Personal Information Act, commencing mid-year (Moyo, 2020). Concerns over election hacking will still present with the US presidential elections (BBC, 2020), and a number of Chinese based apps and websites being banned around the world (Iyengar, 2020). Such events illustrate the need for this journal to discuss such issues and provide solutions to the challenges faced in providing a safe and secure cyberspace.

In this issue of the IJCWT, the following four 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 IJCWT publishes original innovative findings and provides a forum to discuss the ethical, political, legal, management, technical, and social issues relating to security, peace, terrorism, and conflict in cyberspace. This journal focuses on cyber warfare, security and terrorism using examples from around the world. 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. The journal targets researchers, practitioners, academics, government officials, military professionals, and other industry professionals.

In the first article, "Between the Devil and the Deep Blue Sea: Insurgency and Humanitarian Conditions in IDP Camps in Nigeria," Segun Joshua, Samuel Sunday Idowu, and Faith Osasumwen Olanrewaju use a structured questionnaire based on the forced/involuntary migration theory to investigate the linkages between insurgency and internally displaced persons in Nigeria. The conditions in the IDP camps are also considered. They conclude that the primary reason for internal displacement is to seek security from insurgencies, even though the conditions in the camps are poor. Recommendations include increased welfare and security for those residing in the camps.

The second article, titled "Knowledge Extraction on the Nexus Between Terrorism Criteria and Attacks on Private Citizens and Property," is authored by Donald Douglas Atsa'am and Ruth Wario. The authors conduct the knowledge extraction on the Global Terrorism Database to investigate the relationship amongst the criteria for terrorism and attacks against private citizens and/or property. They conclude that these attacks are not indiscriminate, and are strongly related to the intention to coerce, intimidate or publicize to larger audience(s).

The third article, "Social Media: A Protagonist for Terrorism in Nigeria," is authored by Yinka Y Olomojobi, and Odusanya Temitope Omotola. They base their analysis on the grievance model and the dependency model and conclude that social media is a tool that can be used for the counter-terrorism efforts as well as a tool used by terrorist groups.

The fourth and final article by Maximiliano Korstanje, "Tracing the Cultural Background of the Lone-Wolf Terrorism: Dilemmas, Contradictions, and Opportunities for the Next Decade," assesses the roots and implications posed by the perception of modern terrorism based on lone wolf tactics targeting crowded public spaces. He concludes that the change of colonial-style tourism literature change after the 9/11 attacks, which has given rise to the modern narratives and perceptions around terrorism.

Brett van Niekerk
Graem Pye
IJCWT
Editors-in-Chief

REFERENCES

BBC. (2020, September 11). *Russia, China and Iran hackers target Trump and Biden, Microsoft says*. Retrieved October, 17, 2020, from https://bbc.com/news/world-us-canada-54110457

Iyengar, R. (2020, August 13). This is what it's like when a country actually bans TikTok. *CNN Business*. Retrieved October 17, 2020, from https://edition.cnn.com/2020/08/13/tech/tiktok-ban-trump- india/index.html

Melman, Y. (2020, May 25). Iran struck first. 'Israel' retaliated massively. Behind the cyber war rattling the Middle East. *Haaretz*. Retrieved June 1, 2020, from https://www.haaretz.com/israel- news/iran-israel-cyber-war-middle-east-mossad-persian-gulf-port-1.8858292

Montalbano, E. (2020, April 3). Spearphishing campaign exploits COVID-19 to spread Lokibot infostealer. *Threatpost*. Retrieved April 6, 2020, from https://threatpost.com/spearphishing-campaign- exploits-covid-19-to-spread-lokibot-infostealer/154432/

Moyo, A. (2020, September 2). Data from Experian breach dumped on the Internet. *ITWeb*. Retrieved October 17, 2020, from https://www.itweb.co.za/content.KA3WwMdDZeoMrydZ