ECCWS 2021

20th European Conference on Cyber Warfare and Security

24 - 25 June 2021, Chester, UK

Mini Track on Modelling Nation-state Cyber-operations

Mini Track Chair: Brett van Niekerk & Trishana Ramluckan, University of KwaZulu-Natal, South Africa

Cyber operations have been evolving since the Stuxnet infection of the Natanz nuclear facility became public. There has been reported outages of Ukrainian power grids due to cyber-attacks, a reported Israeli airstrike retaliating against a building housing Hamas cyber capability and US cyber-attacks against Iranian air-defence networks. The WannaCry and NotPetya malware were attributed to state-backed actors. It is clear that "coercive cyber capabilities are becoming a new instrument of state power, as countries seek to strengthen national security and exercise political influence. Military capabilities are being upgraded to monitor the constantly changing cyber domain and to launch, and to defend against, cyber attacks" (IISS, 2014). The World Economic Forum's The Global Risks Report 2020 (WEF, 2020) lists cyber-attacks in the top 10 risks for both likelihood and impact. Despite this rapidly growing concerns over the use of cyber-operations, some challenges and questions still have not been resolved after 10 years of discussion, including accepted international legal frameworks and models of state behaviour in projecting and defending national power online.

- Models of national cyber-power
- Mathematical and technical models of national cyber-operations and decision making
- International law and legal frameworks applied to national cyber-security, cyber-warfare and cyber-espionage
- International relations models applied to cyber security, cyber warfare and cyber espionage
- Command and control and intelligence models for cyber-operations
- Modelling of nation-state and state-sponsored threat actors
- Case studies of international cyber-security incidents and cyber-attacks
- Closing the gap between technical and policy perspectives

Dr Brett van Niekerk is a senior lecturer in computer science at the University of KwaZulu-Natal. He serves as chair for the International Federation of Information Processing Working Group on ICT in Peace and War, and the co-Editor-in-Chief of the International Journal of Cyber Warfare and Terrorism. He has numerous years of information/cyber-security experience in both academia and industry, and has contributed to the ISO/IEC information security standards. In 2012 he graduated with his PhD focusing on information operations and critical infrastructure protection. He is also holds a MSC in electronic engineering and is CISM certified.

Dr Trishana Ramluckan is a Postdoctoral Researcher in the School of Law and an Adjunct Lecturer in the Graduate School of Business at the University of KwaZulu-Natal. She is a member of the IFIP working group on ICT Uses in Peace and War, the Institute of Information Technology Professionals South Africa and is an Academic Advocate for ISACA. In 2017 she graduated with a Doctor of Administration specialising in IT and Public Governance and in 2020 she was listed as in the Top 50 Women in Cybersecurity in Africa. Her current research areas include Cyber Law and Information Technology Governance.

Submission details

In the first instance a 300-word abstract is required, to be received by **2nd of December 2020.** Please read the guidelines at http://www.academic-conferences.org/policies/abstract-guidelines-for-papers/

Submissions must be made using the online submission form at
http://www.academic-conferences.org/conferences/eccws/eccws-abstract-submission/
If you have any questions about this track please email: ramluckant@ukzn.ac.za or VANNIEKERKB@ukzn.ac.za

See more about ECCWS at *http://www.academic-conferences.org/conferences/eccws/*