acpi

ECCWS 2023

22nd European Conference on Cyber Warfare and Security
22-23 June 2023, Athens, Greece

Mini Track on Offensive Cyber-operations: Multi-disciplinary perspectives

Mini Track Chairs: Brett van Niekerk (Durban University of Technology, South Africa) &
Trishana Ramluckan (University of KwaZulu-Natal, South Africa)

Offensice cyber operations have been evolving since the Stuxnet infection of the Natanz nuclear facility became public, including reported outages of Ukrainian power grids due to cyber-attacks and reported Israeli retaliation against an Iranian port. 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. Researchers such as Smeets (2022) challenge the perception that offensive cyber capability is an equaliser, and the 2022 Russia-Ukraine conflict has divided experts on the role of offensice cyber operations in traditional conflict. Therefore, there is a need to engage in research and discussion on offensive cyber operations from multi-disciplinaty perspectives.

- Case studies of offensive cyber-operations
- Diffusion of offensive cyber capabilities
- Models of national cyber-power
- Command and control, intelligence, and targeting for cyber-operations
- Cyber-weapons
- International law and legal frameworks applied to offensive cyber-operations
- Offensive cyber-operations in international relations and diplomacy
- Modelling of nation-state and state-sponsored threat actors
- Closing the gap between technical and policy perspectives on offensive cyber-operations

Dr Brett van Niekerk is a senior lecturer in information technology at the Durban University of Technology. 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 Honorary Researcher in the School of Law at the University of KwaZulu-Natal and Research Manager at Educor Holdings. 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, 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: brettv@dut.ac.za or ramluckant@ukzn.ac.za

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