

ICCWS 2021

16th International Conference on Cyber Warfare and Security

25-26 February 2021, Tennessee, USA

Mini Track on The double-edged sword of Artificial Intelligence in Cyber Warfare

Mini Track Chair: **Pardis Moslemzadeh Tehrani**, University of Malaya, Kuala Lumpur, Malaysia



Information warfare is a key point in winning any world conflict and has led states to seek the benefits of emerging technologies. In the context of warfare, artificial intelligence (AI) is rapidly becoming the center of a global power play. It is leading societies towards a new algorithm of warfare that knows no boundaries or borders and is well on its way to revolutionize warfare. The trend is leading to nations continuing to develop the AI automated weapons system.

As seen in the past year, cyber-attacks powered by artificial intelligence has become a real threat with the first AI-powered cyber-attack was detected in India last year. And expectations are that these attacks will continue to grow in threat level and regularity and preventing them will become more problematic. The use of AI and machine learning in cyber operations opens a range of dangerous scenarios from the use of AI-powered autonomous weapons in cyber warfare to AI-machine learning methods for conducting offensive cyber warfare. AI in cyber warfare is a double-edged sword as it can be used both offensively and defensively. Machine learning and automation have become necessary tools of states to defend themselves as well as to launch attacks on other states.

AI powered autonomous weapons pose a great threat and can be worse than traditional computer viruses as they employ military means of identifying and engaging targets without human intervention. Developments in AI autonomous weapon systems (AWS) pose complex security challenges. Such emerging technology will shape and transform the conduct and consequences of cyber warfare and impact national security and defence systems as well as lead to the proliferation of violence and humanitarian responses.

Topics of interest include, but are not limited to:

- Artificial intelligence as a dual technology in cyber warfare
- AI algorithm in cyber attack
- The ethical and cyber security issues of AI in cyber warfare
- Armed drone and Autonomous weapon in warfare
- New Warfare Technologies
- The legality of new weapons in cyber warfare under IHL



Pardis Moslemzadeh Tehrani is a senior lecturer at the Faculty of Law, University of Malaya. Her research interests lie in the areas of cyberterrorism, cyberlaw, and international humanitarian law. Pardis's research has been widely published in peer-reviewed journals and she has presented papers at national and international level conferences. She is a member of the editorial review board in several journals. She is also an international scientific member of the Australian and New Zealand Society of International Law. Pardis's most recent book is *Cyberterrorism: The Legal and Enforcement Issues* (World Science and Imperial College Press of London, 2017).

Submission Details

In the first instance a 300-350 word abstract is required, to be received by the **5th August 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/iccws/iccws-abstract-submission/>

If you have any questions about this track please email: Pardismoslemzadeh@um.edu.my

See more about ICCWS 2021 at <http://www.academic-conferences.org/conferences/iccws>