

Topic 1: Computational Intelligence in Cybersecurity.

Computational Intelligence (CI) constitutes an umbrella of techniques, has proven to be flexible in solving dynamic and complex real-world problems. These techniques typically include Machine Learning, Fuzzy Logic, Evolutionary Computation, Intelligent Agent Systems, Neural Networks, Cellular Automata, Artificial Immune Systems, Game Theory and other similar computational models. Cyber defense is a continuously changing attack landscape as the software/hardware components are added and/or updated more frequently at different layers of cyber systems for additional functionalities and/or improved usability while in many cases these are not security-enabled. Attackers exploit these vulnerabilities and find attack paths to compromise the target systems.

In this talk, I will discuss multi-faceted Computational Intelligent (CI) techniques which can provide an efficient security paradigm to deal with influx of new threats in network infrastructures and smart applications. I will cover some CI approaches which are used to augment defense-in-depth and building zero-trust architectures and to add necessary security enhancements to the design, development, testing and operation of cyber-enabled systems.

References:

- IEEE Symposium Series on Computational Intelligence (SSCI)-CICS, organizer: Dr. D. Dasgupta, since 2007.
- Machine learning in cybersecurity: a comprehensive survey. D Dasgupta, Z Akhtar, S Sen. The Journal of Defense Modeling and Simulation, 2020. <https://doi.org/10.1177/1548512920951275>.