Proceedings of the 4th Annual World Conference
of the Society for Industrial and Systems Engineering,
Fort Lauderdale, Florida, USA
October19-21, 2015

Cyber Threat Identification and Mitigation

T.K. Bardhan and G. Jones

Department of Industrial and Systems Engineering
Morgan State University
Baltimore, MD 21251, USA

Corresponding author's Email: garfield.jones@morgan.edu

Author Note: Dr. Tridip K Bardhan is currently serving as the Chairperson of the Industrial and Systems Engineering Department at Morgan State University. Garfield Jones is a doctoral candidate in the Industrial and Systems Engineering department at Morgan State University in Baltimore. Mr. Jones would like to thank Mr. Chad Baer for his support of this research in preparation for this paper.

Abstract: Considerable research has been conducted on neural networks and their relevance to identification of cyber threats. The frequency and intensity of cyber-attacks have grown significantly in recent years. The time to detection and mitigation of these cyber threats have allowed for more types of Distributed Denial-Of-Service (DDOS), password, and malware attacks to manifest without an organization having any awareness of their presence. Government organizations in conjunction with the private sector has been researching and developing applications using cognitive neural networks to assist in the detection, mitigation, and eventually the prediction of several types of cyber-attacks. The overall goal of this paper is to demonstrate the operation of a fractal neural network and its benefits towards detecting and mitigating specific cyber threats.

Keywords: Cyber Treats, Fractal Artificial Neural Network, Self-Organizing Map (SOM), KOCH Curve