Cyber Threat Intelligence and Adversarial Risk Analysis

These days cyber security and forensic specialists are supposed to detect, analyze and defend against many cyber threats under real-time conditions. Timely dealing with such a huge number of attacks is not possible without employment of artificial intelligence and machine learning techniques. When a significant amount of data is collected from or generated by different security monitoring solutions; intelligent big-data analytical techniques are necessary to mine, interpret and extract knowledge of those data. The emerging field of cyber threat intelligence is investigating applications of artificial intelligence and machine learning techniques to perceive, reason, learn and act intelligently against advanced cyber attacks.

This Special Issue will focus on cutting-edge research from both academia and industry, with a particular emphasis on providing wider knowledge of the field, novelty of approaches, combination of tools and so forth to perceive, reason, learn and act on a wide range of data collected from different cyber security and forensics solutions. Specifically, this Special Issue welcomes three categories of papers: (1) invited articles from qualified experts; (2) contributed papers from an open call with the list of addressed topics, and (3) Selected Papers from the 19th IEEE International Conference on Pervasive Intelligence and Computing (PICom 2020), 6th IEEE International Conference on Cloud and Big Data Computing (CBDCom 2020), and from the 2020 IEEE Cyber Science and Technology Congress (CyberSciTech 2020) which will be held June 22-26, 2020 in Calgary, Canada

Topics of interest include but are not limited to:

- Application of machine learning tools and techniques in cyber security and cyber forensics
- Threat intelligence techniques for constructing, detecting, and reacting to advanced intrusion campaigns
- Applying machine learning tools and techniques for malware analysis and fighting against cyber crimes
- Intelligent analysis of different types of data collected from different layers of network security solutions
- Threat intelligence in cyber security domain utilising big data solutions such as Hadoop
- Intelligent methods to manage, share, and receive logs and data relevant to variety of adversary groups
- Interpretation of cyber threats and forensic data utilising intelligent data analysis techniques
- Generate intelligence of existing cyber security data generated by different monitoring and defence solutions
- Automated and intelligent methods for generation of adversary groups profile
• Automated integration of analysed data within incident response and cyber forensics capabilities

All submitted papers will be reviewed by at least three independent experts to assure their originality, readability and relevance. We will also recommend submission of multimedia with each paper as it significantly increases the visibility, downloads, and citations of articles.

**Important Dates:**
- Paper submission due: August 31st, 2020
- First-round acceptance notification: October 31, 2020
- Revision submission: December 1, 2020
- Notification of final decision: January 15, 2021
- Submission of final paper: February 15, 2021
- Publication date: 2nd quarter of 2021

All the papers should be formatted in the standard Evolutionary Intelligence format. See the Instructions for Authors at the Journal’s homepage. All submissions should be submitted through online submission system of Evolutionary Intelligence.

**Guest Editors**

1. **Dr. Ali Dehghantanha**, Director, Cyber Science Lab, School of Computer Science, University of Guelph, (IEEE Senior Member) Ontario, Canada, [https://www.uoguelph.ca/computing/people/ali-dehghantanha](https://www.uoguelph.ca/computing/people/ali-dehghantanha) E-mail: adeghhan@uoguelph.ca

2. **Dr. Reza M. Parizi**, College of Computing and Software Engineering, Kennesaw State University, GA, USA (IEEE Senior Member) [http://facultyweb.kennesaw.edu/rparizi1/index.php](http://facultyweb.kennesaw.edu/rparizi1/index.php) E-mail: rparizi1@kennesaw.edu

3. **Dr. Yang Xiao** (IEEE Senior Member), The University of Alabama, USA [yangxiao@ieee.org](mailto:yangxiao@ieee.org) [https://dblp.uni-trier.de/pers/hd/x/Xiao:Yang](https://dblp.uni-trier.de/pers/hd/x/Xiao:Yang)

4. **Dr. Gautam Srivastava**, Associate Professor, Computer Science, Brandon University, Canada (IEEE Senior Member) [https://people.brandonu.ca/srivastava/](https://people.brandonu.ca/srivastava/)
https://scholar.google.ca/citations?user=qk9hEQoAAAAJ&hl=en&oi=ao

E-mail: srivastavag@brandonu.ca