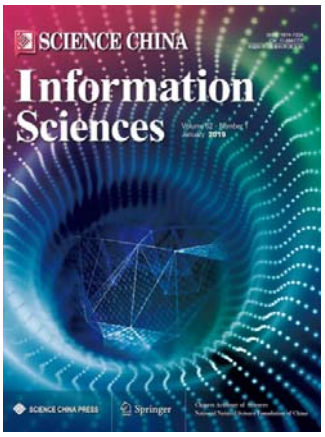
# Call for Paper

## Special Focus on Cyber Security in the era of Artificial Intelligence




Over the past decade, the rise of Artificial Intelligence (AI) and machine learning (including deep learning) algorithms has dramatically increased the capability of attackers and the attack surface of critical systems. A large number of machine learning algorithms have been studied in both academia and industry to enhance the security of the cyberspace through, for instance, identifying malicious network traffic, improving intrusion detection systems, or enhancing malware detection. Meanwhile, it has also been widely recognized that AI and machine learning algorithms are vulnerable to various security and privacy threats: Adversarial examples can mislead the model to output incorrect predictions. Poisoning the training data may result in incorrect models with trapdoors. The privacy of training data and model parameters can be severely compromised by inference attacks and reverse engineering of models. This special issue calls for the cutting-edge contributions and progress on integrating artificial intelligence and cybersecurity together from both academia and industry. The main purpose of this special issue is to publish the state-of-the-art solutions, challenges, and future trends with a particular emphasis on the field of artificial intelligence and cybersecurity, including but not limited to:

- AI for enhanced security and privacy
- AI for critical infrastructure security
- AI for IoT security and privacy
- AI for network security
- AI for system security
- AI for anomaly and intrusion detection
- AI for malware analysis and detection
- AI for data security and privacy
- Data-driven access control
- Adversarial machine learning
- Threat and attack model generation based on machine learning
- Adversarial examples: attacks and defenses
- Data poisoning: attacks and defenses
- Privacy-preserving training and inferences
- Backdoors in AI models
- Federated learning
- AI Security with specialized hardware

**Submission:**

The papers should be edited in the SCIS template, and should be submitted online through the manuscript submission system of *SCIENCE CHINA Information Sciences* (**Impact Factor: 3.304**). The submission website is: https://mc03.manuscriptcentral.com/scis. You should choose **Special Focus on Cyber Security in the era of Artificial Intelligence**. Information and guidelines on preparation of manuscripts are available on the journal website: http://scis.scichina.com.

**Important Dates:**

Manuscript submission deadline: **2021/9/1**

Revision notification: 2021/12/1

Final manuscripts due: 2022/3/1

Publication: 2022/6/1

**Guest Editors:**

Elisa Bertino, Purdue University, United States, bertino@purdue.edu

N. Asokan, University of Waterloo, Canada, asokan@acm.org

Zhenkai Liang, National University of Singapore, Singapore, liangzk@comp.nus.edu.sg

Xinsheng Ji, China National Digital Switching System Engineering & Technological R&D Center, jxs@ndsc.com.cn

Xiaofeng Tao, Beijing University of Posts and Telecommunications, taoxf@bupt.edu.cn

Qi Li, Tsinghua University, China, qli01@tsinghua.edu.cn

Kui Ren, Zhejiang University, China, kuiren@zju.edu.cn