ID: **P4.3-123** Type: **E-poster**

An Expanding Counter-AI Matrix: Whither the Satellite Remote Sensing Revolution?

Satellite remote sensing is a commonly utilized tool for arms control and nonproliferation missions. Lately, there has been growing interest in integrating AI into satellite remote sensing to improve analytical efficiency. However, this enhancement could compromise accuracy and system security due to the susceptibility of AI models to counter-AI techniques. The present research delves into the emerging threats posed by counter-AI to AI-driven satellite remote sensing analysis. It will assess four threat scenarios – data poisoning, model evasion, data inference, and model extraction. Potential counter-AI attacks encompass a range of adversarial AI techniques, spanning from the digital to the physical world, giving rise to security concerns in international and nuclear security. To address this, this article proposes a comprehensive defense framework comprising six essentials: access and quality control of data and models, robustness enhancement of the frameworks, monitoring capability improvement of the satellite remote sensing systems, knowledge and awareness enhancement of humans, adaptability improvement of the risk management, and resilience planning for contingencies.

E-mail

hejingjie@cass.org.cn

In-person or online preference

Primary author: Ms HE, Jingjie (Chinese Academy of Social Sciences)

Presenter: Ms HE, Jingjie (Chinese Academy of Social Sciences)

Session Classification: P4.3 Use of enabling Information Technologies

Track Classification: Theme 4. Sustainment of Networks, Performance Evaluation, and Optimization: T4.3 Use of enabling Information Technologies