

**Research direction:** augment Video Predictive Model with ideas of adversarial attack and defense

**Explanation of attack and defense on deep learning:**

Core idea: deep learning has a different sensitivity than human

Deep network attack: put a black dot on a light sheet

Defend: detect what changes on a light sheet

Attack neural network under test environment strategically to test the robustness of the network