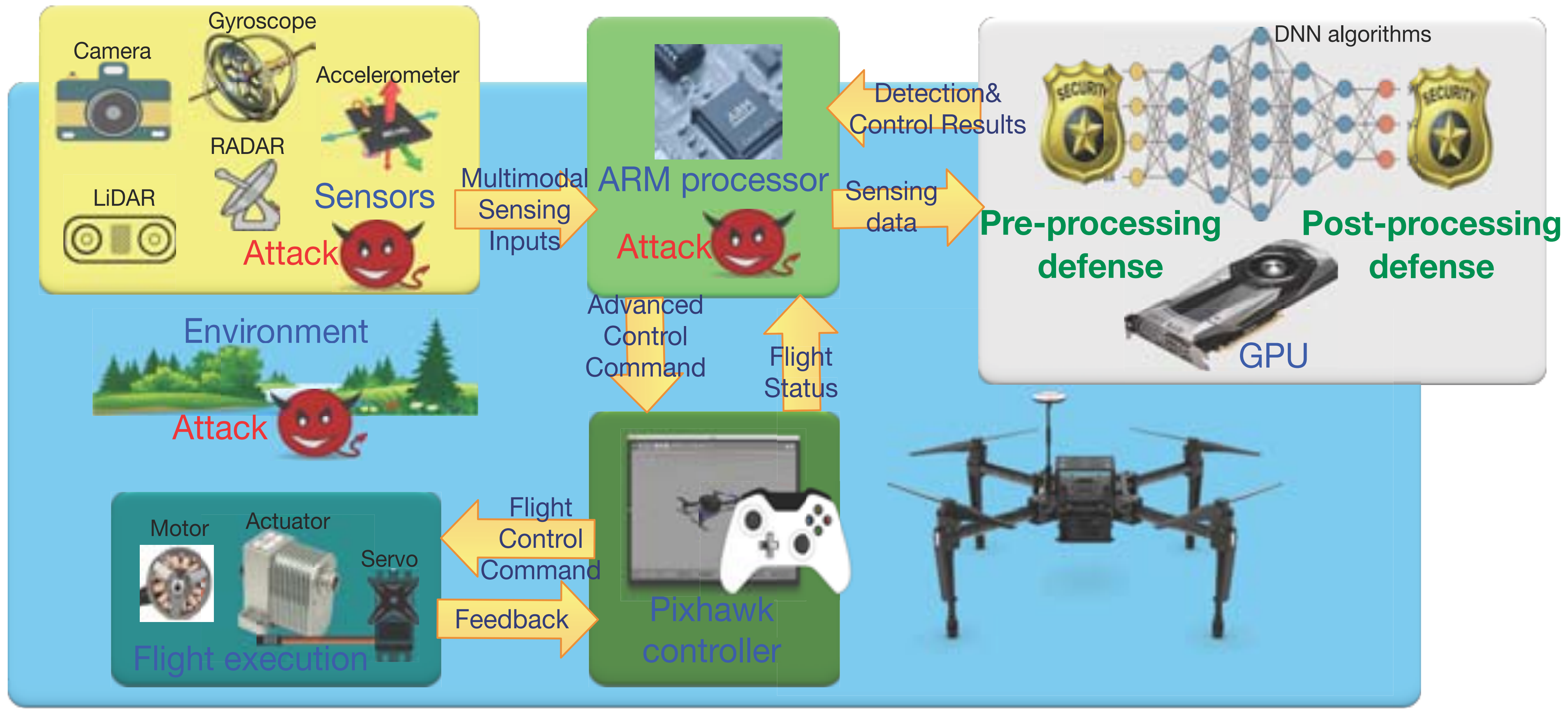
2022 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS’ MEETING

SecureNN: Design of Secured Autonomous Cyber-Physical Systems Against Adversarial Machine Learning Attacks

(CNS-1932351 & CNS-1932464, Nov. 2019 -- Oct. 2023, Xue Lin (Northeastern University), Qi Chen (UC Irvine)

Challenge:

- Multi-model sensing and deep learning based perception and control form the backbone of autonomous CPS, but also bring in new security challenges.



Scientific Impact:

- Advance state-of-the-arts on autonomous systems, AI, security
- Translational to other domains involving deep learning and ubiquitous sensing

Solution:

- Propose a comprehensive threat model of autonomous CPS, where adversarial attacks may be injected (i) from physical world, (ii) by hacking the software/hardware of sensors, and (iii) hacking the ARM processor that coordinates the communications
- Propose a series of security benchmarking and defense techniques

Broader Impact:

- Enhance economic opportunities via solutions that support adoption of AI into security-critical application domains
- Of interests to industrial companies and other government agencies
- Provide unique research training opportunities for graduate/undergraduate students, develop new courses