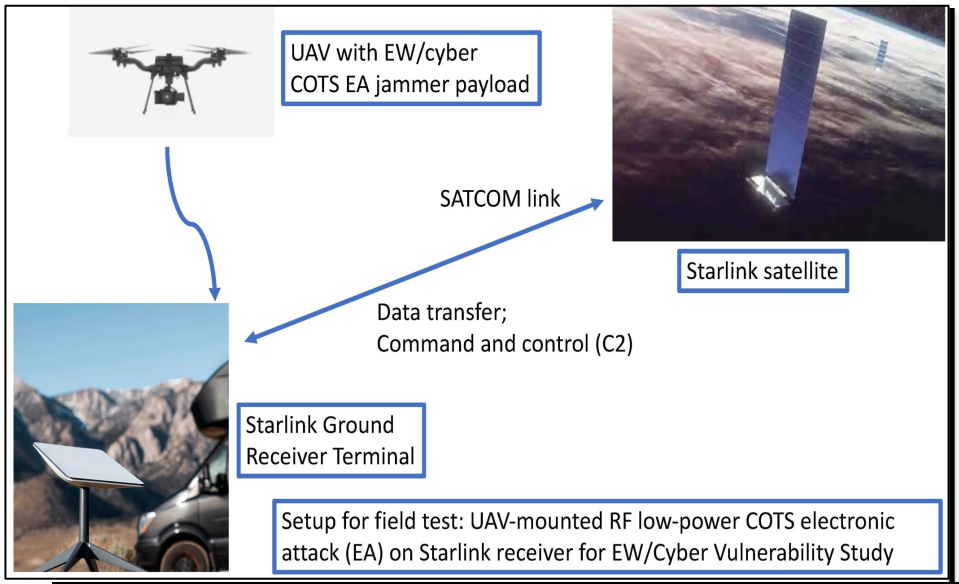
UAV-mounted COTS Electronic Attack of Starlink Ground Receiver for EW/Cyber Vulnerability Study

CRUSER
Consortium for Robotics and Unmanned Systems Education and Research



Problem Statement

- To evaluate EW/cyber vulnerability of Starlink SATCOM downlink receiver from a small form factor, low-weight, and low-power electronic attack (EA) RF emitter with COTS (commercial-of-the-shelf) hardware as payload to small UAV as viable alternative to large, expensive, high-power standoff (non-moving) jammers
- **APPROACH:**
  - Design a small form factor RF emitter from COTS hardware
  - Use of UAV (already in NPS inventory) to carry EA payload as moving alternative to non- or slow-moving jammer platforms

Impact

- This project evaluates the vulnerability of Starlink receiver downlink to EA attack from a UAV
- Specifically, the study will test the robustness of the Starlink terminal downlink communications (for command and control)
- Theoretical performance metrics are analyzed (such as bit rate or data rate)
- Success is measured via experimentation and field tests to report effects on parameters: data rate, latency, etc.

Transition

- PI has on-going research study with NAVSEA PMA-234 who is very interested in deployable EW/EA airborne systems and **more importantly strong NPS student participation**
- NAVSEA has continually supported EW-related UAV implementation and field experiments with PI at NPS
- PI has involvement with AFRL project very interested in EW/Cyber effects on networks (application specific)
- AFRL has funded EW/Cyber efforts in FY23 (and possibly beyond)

PI: RIC ROMERO, ELECTRICAL AND COMPUTER ENGINEERING DEPT.