Cyber Deception in the Flight Deck: A Pilot-Centered Study of Cyber-Physical Resilience

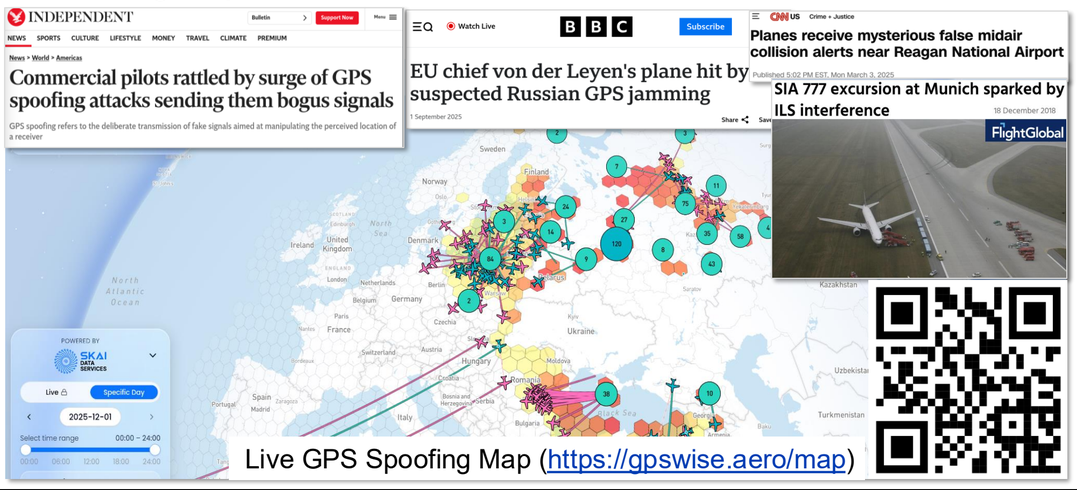
Problem Statement and Goals

Cyber-physical disruptions (e.g., GPS spoofing) are increasingly affecting operational aircraft, forcing pilots to manage unexpected and ambiguous failures that directly threaten flight safety

Current mitigation efforts emphasize technical solutions, while pilots lack standardized, evidence-based procedures to detect, interpret, and respond to cyber-induced anomalies in real time

There is little empirical data on how available detection and mitigation strategies influence pilot workload, task saturation, situational awareness, and decision-making under operational stress

This work generates human-in-the-loop evidence to evaluate mitigation strategies and inform pilot procedures and training for cyber-physical resilient flight operations



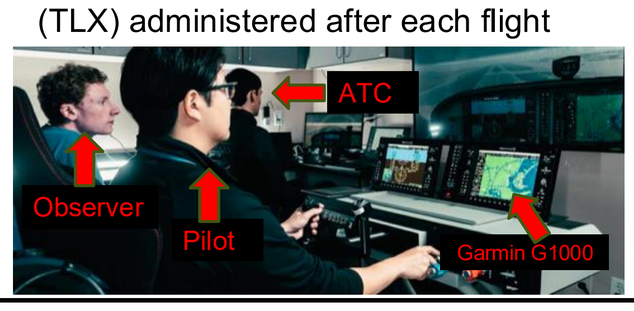
Approach

37 instrument-rated pilots flew instrument approaches in an immersive flight simulator equipped with Garmin G1000 avionics

Scenarios
- Control: Instrument approach with no cyber disruption
- Cyber-physical attack causing deviation from published approach path:
  - GPS database attack
  - ILS spoofing attack

Experimental Groups: Participants assigned to one of four groups
- No Warning: No indication of deviation provided
- Electronic Flight Bag only: Aircraft position overlaid on approach plate
- Air Traffic Control Only: Audible “off-course” warning from simulated ATC
- Both: Combined EFB display and ATC audible warning

Data Collected
- Detection/Response Success: Recognition of the attack and initiation of appropriate corrective action
- Pilot Workload: NASA Task Load Index (TLX) administered after each flight



Results

Attack Recognition Improves with Visual and Auditory Cues
Percentage of pilots recognizing the attack by alerting condition:
- <10% — No warning (baseline);
- 30% — EFB visual only
- 68% — ATC audible warning only;
- 83% — Combined ATC audible + EFB visual (8x increase compared to No Warning!)

Attack recognition improves on second exposure, indicating rapid experiential learning.

Compared to ILS spoofing, GPS attacks are more covert and operationally hazardous.

Productive Workload Enables Improved Cyber-Physical Attack Recognition
- NASA TLX results show increased mental, temporal, and effort demands under alerting conditions relative to the no-warning baseline.
- Despite higher workload, alerting conditions yielded the highest self-reported performance and attack recognition rates, indicating a productive workload–performance tradeoff rather than cognitive overload.

Limits and Next Steps
- Subjective workload measures cannot reveal how recognition improves with exposure, how pilots allocate attention or distinguish effective cross-checking from performance-degrading overload under cyber deception.
- Eye tracking and biometric sensing are needed to identify pilot tactics, techniques, and procedures, attention allocation, and stress responses during cyber-physical attacks.
- Ongoing work expands scenarios to include TCAS spoofing and GPS spoofing with an operationally proposed checklist, plus eye tracking and biometrics at key decision points.

Acknowledgements: I would like to extend my sincerest thanks to ERAU Prescott alumni, Adam Shapiro, and Dr. Krishna Sampigethaya, for their support in this project. This work was supported by the U.S. Department of War Cyber Service Academy (CSA) Grant, Award No. HQ00342410045P00001, and NSF Scholarship for Service (SFS) Grant 2520181. The views and conclusions contained herein are those of the authors and do not necessarily represent the official policies or positions of the Department of War, the National Science Foundation, or the U.S. Government.

Nathan Johnson
Embry-Riddle Aeronautical University
EMBRY-RIDDLE Aeronautical University PRESCOTT, ARIZONA

Cyber Deception in the Flight Deck: A Pilot-Centered Study of Cyber-Physical Resilience

Abstract

Aviation safety is becoming increasingly threatened by cyberattacks such as GPS spoofing and jamming. Aircraft communication, navigation, and surveillance systems are often targeted by nation-state actors, but the impacts of these attacks are often difficult or impossible to limit to specific targets and are affecting civilian aircraft on a near daily basis near areas of active conflict.

While the risks posed by cyberattacks are well known, the aviation industry currently has a lack of guidance for pilots on the safest way to respond to a cyberattack in flight. The aviation industry has been focused on developing much-needed technical solutions to cyber vulnerabilities but has been unclear on what measures can be taken by pilots in the meantime. There is little empirical data on how pilots respond to real world cyberattacks. There is also limited data on how pilot workload is affected by cyberattacks, and if some mitigation strategies might lead to pilots becoming task saturated when performed in real-time operations.

For these reasons, we developed an experimental study to assess pilots' responses to simulated in-flight cyberattacks. Instrument-rated pilots were invited to participate in the study consisting of three instrument approach flight scenarios in an immersive flight simulator including a Garmin G1000 avionics system. Participants first flew a control approach with no cyberattack. The pilots then flew two more approaches on which they would experience either a GPS attack or an ILS spoofing attack. Both attacks would lead the aircraft off course if no corrective action was taken by the pilots. Depending on the experimental group, participants received either no warning, an electronic flight bag (EFB) showing the aircraft's position overlaid on the approach plate, an audible warning by ATC that the aircraft appears to be off course, or both. The flight was recorded as successful if the pilot recognized the cyberattack and took corrective action. Pilots were also asked to complete the NASA Task Load Index survey after each flight to measure self-reported workload factors.

The results of the study indicate that pilots are much more likely to recognize a cyberattack and take corrective action if they have some warning or information to confirm that the aircraft's systems are in error. Fewer than 10% of pilots recognized the cyberattack without any warning. That figure increased to 30% when an EFB was provided without an ATC warning and increased to 68% with an ATC warning and no EFB provided. 83% of pilots successfully recognized the cyberattack when provided with both an audible warning from ATC and an EFB showing the aircraft's position overlaid on the approach plate.

The NASA Task Load Index results indicate that having only one warning (EFB or ATC) increases pilot workload relative to the "no warning" group while simultaneously increasing the chance of successful recognition of the attack as well as self-reported pilot success level. This is also true for the case where pilots receive both warnings. Workload factors in this case are higher than in the cases of just one warning, but success level is also increased.

The next iteration of the study is already underway. Improvements include the addition of a TCAS (Traffic Collision Avoidance System) spoofing scenario as well at the use of a proposed GPS spoofing response checklist. For data collection, digital eye-tracking glasses to record instrument scan pattern and potential fixation, as well as an ECG heart rate monitor to better quantify pilot stress level.

Nathan Johnson
Embry-Riddle Aeronautical University

EMBRY-RIDDLE Aeronautical University PRESCOTT, ARIZONA