



Countering Aviation Security Ecosystem Threats (CASET)

CASET teaches an overview of five major threats to commercial aircraft and the aviation ecosystem. These threats are categorized as either high-technology or low-technology and can disrupt, disable, or destroy commercial aircraft and the infrastructure that supports their safe operation. CASET gives participants an introductory level understanding of these threats, how they are deployed, and steps that can be taken to identify and prioritize efforts to mitigate them. The threats addressed in CASET are:

- Man-Portable Air Defense Systems (MANPADS) and Anti-Tank Guided Missiles (ATGM)
- Low-Technology Materials and Tactics
- Unmanned Aerial Systems (Drones)
- Cyber Threats
- The Insider Threat

Man-Portable Air Defense Systems (MANPADS) and Anti-Tank Guided Missiles (ATGMs)

MANPADS and ATGMs are military weapons that can be effectively used to destroy civilian and military aircraft. There have been numerous MANPADS attacks against civilian aircraft in the past 40 years, and ATGMs have been used against stationary military aircraft. Participants will learn to identify the most proliferated MANPADS and ATGM systems outside of regulatory control around the world and to record and report the identifying information off them to aid in international efforts to prevent the potential for these weapons to be used against civilian aircraft.



Low-Technology Materials and Tactics

Civilian aircraft are vulnerable to terrorists bringing low-technology materials on board an aircraft to cause chaos, death, or even total destruction in flight because of the unique characteristics of civilian aircraft, such as confined space, limited airflow, and an inability to escape. Participants will receive an introduction to the chemical and biological materials, technologies, and tactics that make a low-technology attack possible, and how these materials can be manipulated in new and creative ways to bypass security and bring them onboard an aircraft.

Unmanned Aerial Systems (Drones)

Unmanned Aerial Systems and Vehicles (UAS and UAV) are increasingly used by non-state actors to conduct terrorist attacks. CASET will raise awareness of the UAS and UAV threat to civil aviation, current drone attack methods and evolving tactics that civil aviation security officials should be aware of, and counter-drone operations. Information will include a focus on gaps in knowledge, security steps to mitigate the UAS and UAV threat, and how to prioritize them.



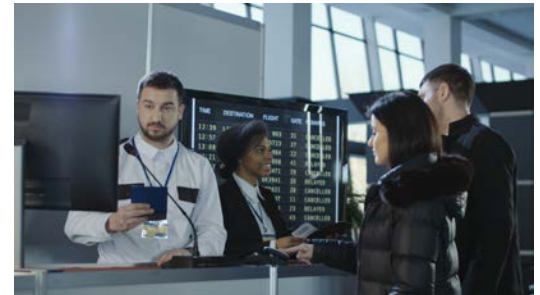
Cyber Threats



Computer and other electronic systems are integral to the operation of the aviation ecosystem, from in-flight controls to passenger ticketing, screening, and airport logistics. Participants will learn about vulnerabilities for manipulation or attack on various systems that air carriers and airports rely on to maintain daily operations and serve their customers. Information learned will help aviation security professionals identify where vulnerabilities may exist in their current cyber dependent systems so that security needs can be identified and prioritized.

The Insider Threat

Airport personnel and staff with nefarious intent and consistent access to internal airport facilities and civilian airliners potentially pose the greatest threat to the security of civilian aircraft. Advances in security detection technology have greatly reduced the ability for outside threats (both materials and people) to affect an aircraft or be introduced into the aviation ecosystem. However, these security enhancements make the “Insider” a high value component of future plots and attacks. Participants will learn principles of insider threats and steps that can be taken to mitigate them.



Course Logistical Details

Course Length: In person – 4 or 5 days. Remote – 8 to 10 days, 2-4 hour instruction blocks

Number of Participants: 25

Number of Instructors: 3-4

Target Audience: Aviation security officials, border security officials, police, and policy makers responsible for protecting civil aviation. The course includes lectures, interactive exercises, and scenario discussions. Training is provided by English speaking instructors assisted by professional translators.

Venue: Large classroom or conference room with tables and chairs where students can receive presentations and participate in group activities. Virtual delivery options available.

Other Requirements: Reliable WiFi access in training room for presentations, flip charts, break area.