Bashar ALOhali

Director - Cyber Security at GACA

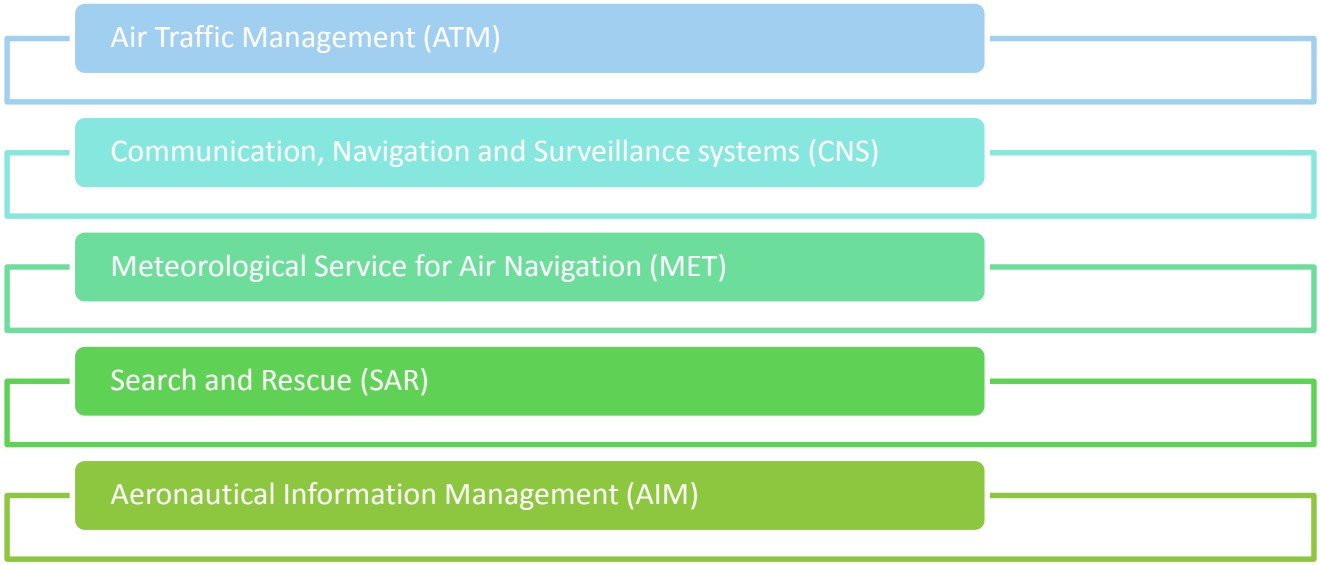
Cyber Security Threat to Air Navigation Service Provider (ANSP)

- Cyber Security - The Term Itself
  - The protection of Allied Hardware, Software and Data from cyber attacks Include the following domains:
    - Unauthorized Access to Programs and Data
    - Protection of Data Centers and Other Systems
    - Protection of Network and communcation

- As per US Department of Homeland Security
- Cyber Threat is defined as
    - Any identified effort directed toward access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority

- Why Cyber Security to be taken seriously
  - Increased use of some new types of cockpit communications, including controller-pilot data link communications (CPDLC), means the cockpit is at a higher risk of hacking or interference than ever before. CPDLC enhances ATC surveillance and intervention capability. It also plays an instrumental role in reducing mid-air collision risk, while also decreasing voice traffic on radio frequencies. But these communications – whether between the cockpit and the ground or between aircraft – are unsecured.

- Domains to Air Navigation Service Provider (ANSP)



- # Threats to Air Navigation Service Provider (ANSP)

System	Ground/Air Dependent	Technology	Dependency	Vulnerability
Primary Surveillance Radar (PSR)	Ground	Measure the bearing and distance of targets using the detected reflections of radio signals	Airplane target independent	Not IT Dependent
Secondary Surveillance Radar (SSR)	Ground	Requests additional info from aircraft like identity, altitude, speed	Targets equipped with transponder	Eavesdropping
Traffic Collision and Avoidance System (TCAS)	Air	Target identity interrogation	Targets equipped with transponder	Eavesdropping, jamming, spoofing
Automatic Dependent Surveillance-Broadcast (ADS-B)	Air	Targets broadcast information about identity, altitude, speed	Targets equipped with transponder	Eavesdropping, jamming, spoofing
Wide Area Multilateration (WAM)	Ground	Combines ADS with RSR and SSR Data for robustness	Central Processing IT based information	Data processing and IT related

- Threats to Air Navigation Service Provider (ANSP) – Other Domains

Communication, Navigation and Surveillance systems (CNS)

- Destruction of Communication with Pilot with Air Traffic Control
- Prone to Hijack if Navigation System fails
- Unable to Monitor the traffic of airplanes

Meteorological Service for Air Navigation (MET)

- Unable to provide correct forecast of weather
- Prediction for and data analysis of volcanic activity will be impaired

Search and Rescue (SAR)

- Unable to pinpoint correct positioning for swift search & rescue

Aeronautical Information Management (AIM)

- Unable to provide correct and timely information
- Sensitive Data Breach threatening complète ASNP

• Cyber-Threats: Network and Communication Attacks

- ANSP networks are considered more vulnerable from malicious sources. These attacks can be categorized into active attacks and passive attacks.
- Different wireless communications can be jammed including of radio signals and air traffic management
- Network and information systems are disrupted to impact the availability of services of ANSP, confidence loss and as a result potential damages.

- Major Cyber Threats in Aviation
  - The infrastructure of the civil aviation consists of systems interconnecting with components therefore increasing the susceptibility for cyberattacks.
  - Could information disrupts and data change causing the pilots to make “wrong decisions” thinking that there is damage to vital systems in aircraft.
  - Information disruptions can cause false representation which can force the pilot to land the aircraft.

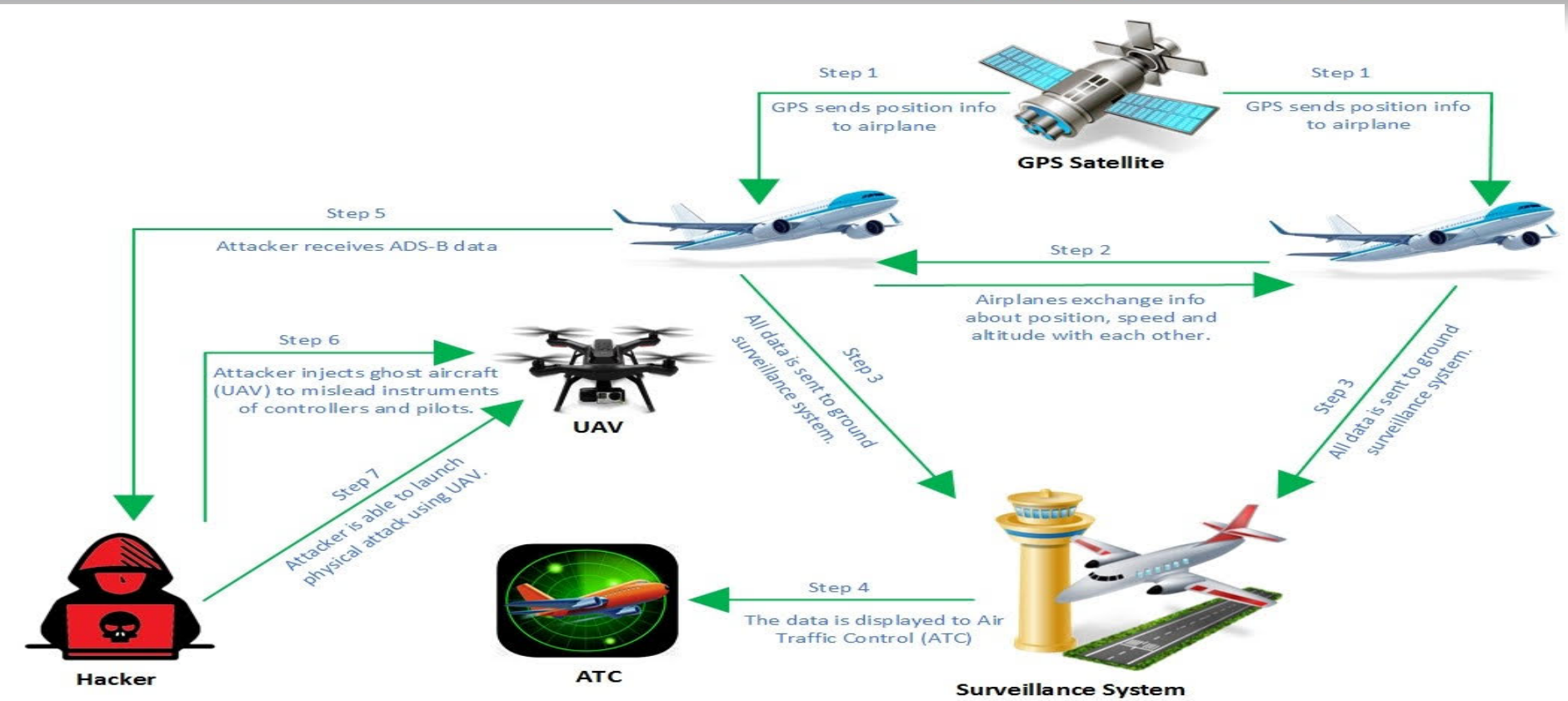
- Major Cyber Threats in Aviation
  - Network and information systems are disrupted to impact the availability of services of ANSP, confidence loss and as a result potential damages.

- ADS-B TECHNOLOGY
  - ADS-B is a technology where an aircraft determines its own position using satellites and then broadcasts that information unencrypted via a radio frequency.
  - Recently there have been concerns about the possibilities of spoofing this technology. This means it is technically possible for someone to broadcast the details of fake aircraft, with obvious safety concerns.

- ADS-B TECHNOLOGY
  - lack of entity authentication to protect against message injection from unauthorized entities.
  - lack of message signatures or authentication codes to protect against tampering of messages or impersonating aircrafts.
  - lack of message encryption to protect against eavesdropping.
  - lack of challenge-response mechanisms to protect against replay attacks.
  - lack of ephemeral identifiers to protect against privacy tracking attacks.

- ADS-B TECHNOLOGY THREATS
  - the new technology of ADS-B enables certain flight-tracking providers to see the aircraft registration information.
  - Many applications are available that enable people to track aircraft all over the world – and very inexpensively.
  - “ADS-B transmits aircraft data in real-time, The data isn’t limited by participation in the BARR program, and there’s no law that prohibits publishing or distributing the data.”

- ADS-B TECHNOLOGY THREATS
  - Denial of service (DoS), e.g., by jamming radio signals, although this is not only specific to ADS-B
  - Threats ADS-B
  - Eavesdropping
  - Spoofing, impersonation
  - Message injection/replay
  - Message manipulation


Step 1
GPS sends position info to airplane
GPS Satellite
Step 1
GPS sends position info to airplane
Step 5
Attacker receives ADS-B data
Step 2
Airplanes exchange info about position, speed and altitude with each other.
Step 6
Attacker injects ghost aircraft (UAV) to mislead instruments of controllers and pilots.
UAV
All data is sent to ground surveillance system.
Step 3
Step 3
All data is sent to ground surveillance system.
Step 7
Attacker is able to launch physical attack using UAV.
Hacker
ATC
Step 4
The data is displayed to Air Traffic Control (ATC)
Surveillance System

- False Alarm
  - False alarm attack works by using the ability of ADS-B technology to send emergency signals to control tower in case of an emergency. The attacker might delete the aircraft's message or modify it to make it look like a case of emergency.

- Recommendations

1. Perform an initial security assessment of the elements supporting air navigation as well as their relationships, in order to identify it vulnerabilities and to ensure adequate protection against future potential attacks and current global threats.

2. Apply controls to existing aviation and air traffic system to detect exposure to attacks and make them cyber secure without having to replace and refit.
   - Certification, legal and liability issues should be taken into account.

- Recommendations

3. Innovate data-sharing architectures capable of connecting and providing access to distributed data while preserving privacy.

4. Adapt mental models within the sector to prepare operators to understand and manage cyber threats.

- Recommendations

5. Requirement of updating software and firmware of IT components in order to fix security vulnerabilities of any critical infrastructure.

6. Deeper study on the security analysis of aviation specific protocol implementations (vulnerabilities, trust, software library).


CYBER SECURITY AND RESILIENCE SYMPOSIUM
TOWARDS A RESILIENT AVIATION CYBERSPACE
AMMAN, JORDAN | 15-17 OCTOBER 2019
ICAO
Thank You