



סייבר ישראל
Cyber Israel

Civil Aviation Cyber Threats

Tom Alexandrovich
Aviation Guidance Manager

Security Vulnerabilities in Next Generation
Air Transportation Systems

NATS

DISCLAIMER

- This presentation is for informational purposes only.
- Do not apply the material if not explicitly authorized to do so
- I'm taking full responsibility whatsoever of applying or experimenting with presented material
- Authors are fully waived of any claims of direct or indirect damages that might arise from applying the material

- **DO NOT TRY THIS AT HOME!**
- **USE AT YOUR OWN RISK!**



Is any one a pilot?





סייבר ישראל
Cyber Israel

Civil Aviation Cyber Security



Civil Aviation Cyber Defense Dept.

Major Cyber Threats in Aviation



סייבר ישראל
Cyber Israel

■ Downing An Airplane

Damage to vital systems for aircraft flying

Disrupting information and changing data that will cause pilots to make "wrong decisions".

Disrupting information that would cause a false representation that would force the pilots to land the aircraft.

■ Disabling The Airport

Airport Closure

Taking control of a system that will cause "public trust" damage.

Cyber Events In Aviation



סייבר ישראל
Cyber Israel

Disruption of GPS systems of unmanned aircraft

Penetration into ground computing systems

Penetration of aircraft systems through a computer interface in the passenger compartment

The screenshot shows a news article from Fox News Insider. The main headline is "Experts: Hackers Could Bring Down Planes Via In-Flight Entertainment System". Below it, there are social media sharing options for Facebook and email. The article is categorized under "SECURITY" and has a sub-headline: "Ground control: Analysts warn airplane communications systems vulnerable to hacking". The author is identified as "Nata Zinnerman". A prominent sub-headline reads: "Hack attack leaves 1,400 airline passengers grounded". The author's name "Arjun Kharpal" and his Twitter handle "@ArjunKharpal" are visible, along with the publication date: "Published 7:24 AM ET Mon, 22 June 2015 | Updated 10:26 AM ET Mon, 22 June 2015". The NBC logo is also present. At the bottom, there is a video player thumbnail with the text "POLISH AIRLINE HACKED" and "Airline passengers stranded after hacking incident", with a timestamp of "12:48 PM ET Mon, 22 June 2015 | 00:30".

Cyber Threats - Airport



סייבר ישראל
Cyber Israel

- ⚠️ Damage to the Runway Lighting System
- ⚠️ Disruption of HBS baggage system
- ⚠️ Disruption of the HVAC system, electricity or parking
- ⚠️ Jamming ramps or sleeves
- ⚠️ Access to physical security systems
- ⚠️ A ransom attack

British Airways cancels all flights from Gatwick and Heathrow due to IT failure

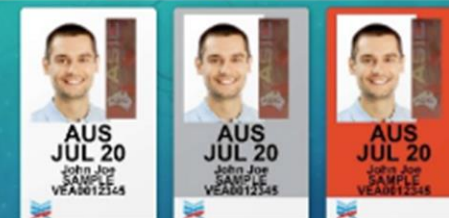
Hundreds of flights at the two airports have been affected, with more around the world suffering major delays

Ukraine's airport, metro system hit by new cyber attacks

REUTERS
KDEV
published
October 24, 2017

DATA BREACH AT AUSTRALIAN AIRPORT IDENTITY SECURITY SYSTEM

Security Newspaper | July 14, 2018 | Data Security | No Comments



AVIATION SECURITY IDENTIFICATION CARD

WHAT IS AN ASIC CARD?
VISIT: [HTTPS://WWW.ASIC.NET.AU/](https://www.asic.net.au/)

CONNECTED AIRCRAFT



סייבר ישראל
Cyber Israel

The
Aircraft Big Data
vector background



Civil Aviation Cyber Defense Dept.

Cyber Threats - Cockpit

Attack vectors based on penetrating aircraft systems

- ⚠ Software update
- ⚠ Communication channels
- ⚠ Updating the EFB



סייבר ישראל
Cyber Israel

Cyber threats - Ground Systems

Attack vectors through ground systems



Operating networks of airlines



Supply chain: software or hardware

NOTICE

**Do Not Remove/Interrupt
Aircraft Power**

Software Installation In-Process







סייבר ישראל
Cyber Israel

Cyber Threats - Passenger Cabin



סייבר ישראל
Cyber Israel

Attack vectors through passenger cabin

-  Disruption of aircraft systems through cabin interfaces
-  Exposure to Improper content in the multimedia system
-  Lack of monitoring or supervision of access points and connection from the passenger cabin
-  Theft of personal information

787 Dreamliner structure suppliers

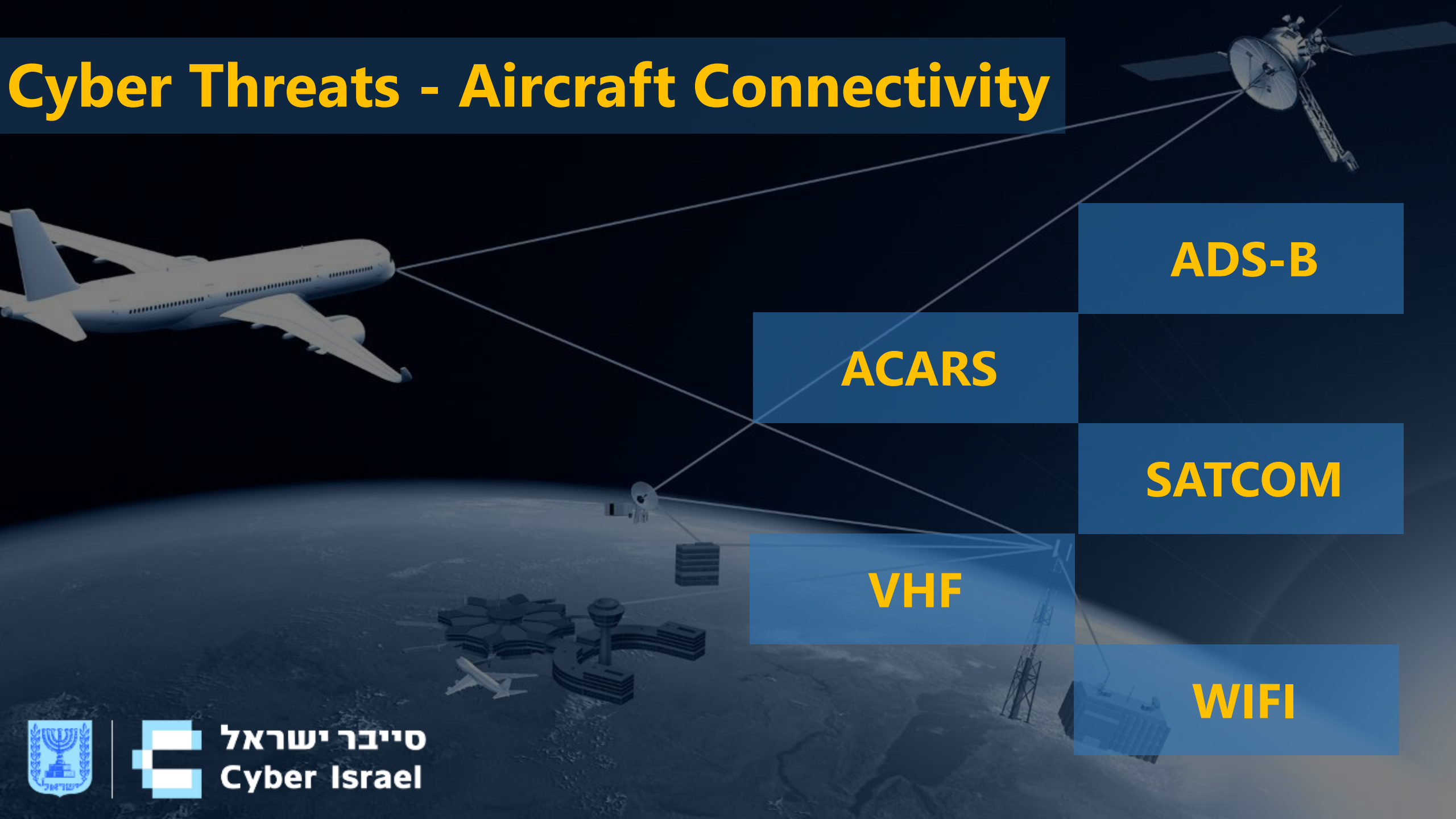
Selected component and system suppliers.



Supply Chain



Cyber Threats - Aircraft Connectivity



ADS-B

ACARS

SATCOM

VHF

WIFI



סייבר ישראל
Cyber Israel

Next Generation Air Transportation System (NextGen)



ICAO
Global Harmonization

Aircraft Trajectory Based Operations

Performance-Based Services

Weather Assimilated into Decision-Making

Air Navigation Operations and Support

Flight Operations and Support

Super Density Operations

Policy & Regulations

Equivalent Visual Operations

Local/State Community

Airport Operations and Support

ADS-B System Functionality



Automatic **D**ependent **S**urveillance-**B**roadcast

ATC of the future (FAA NextGen project)

Required on most AC in US by 2020, required in Europe

Augments primary surveillance radar (ADS-B Out)

Gives pilots their own radar picture (ADS-B In)

Transport layer, not physical (OSI level 4)

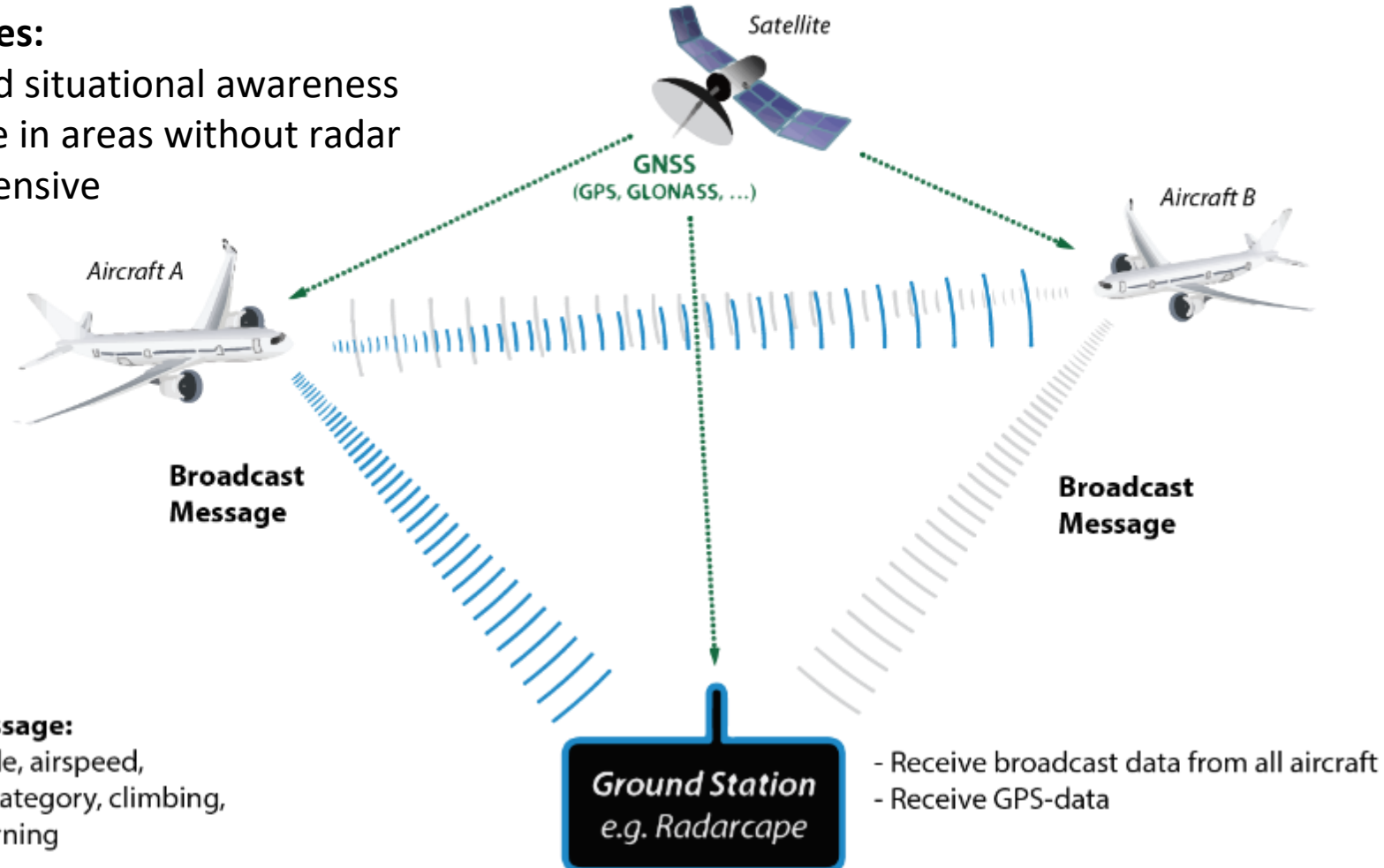
ADS-B System

Automatic Dependent Surveillance Broadcast

- Replacing radar for tracking aircraft worldwide
- Sharing position, altitude, velocity, etc. with air traffic control and other aircraft

Advantages:

- Increased situational awareness
- Coverage in areas without radar
- Less Expensive



Broadcast Message:

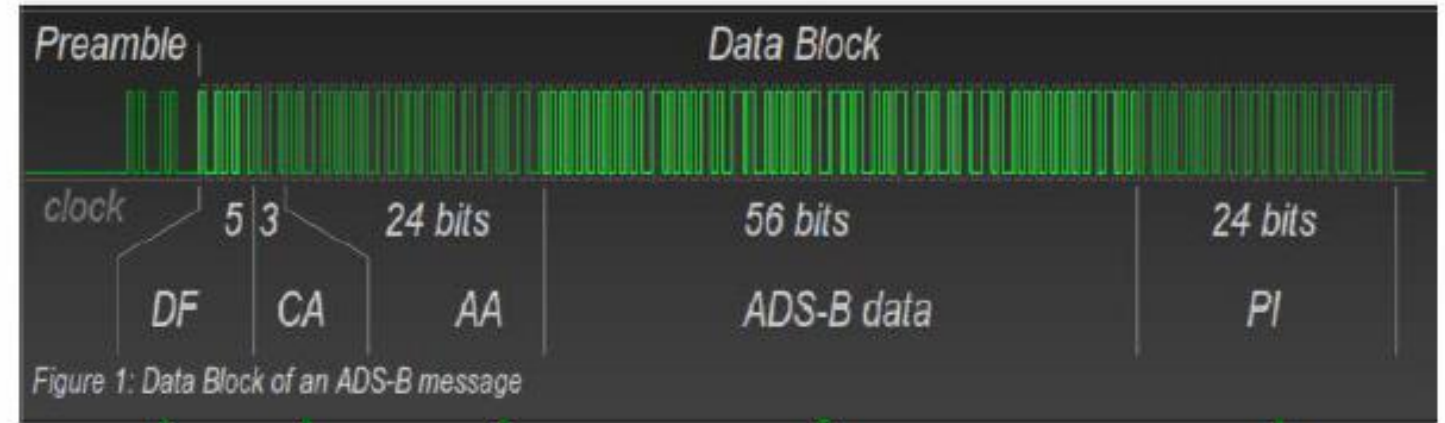
Position, altitude, airspeed, identification, category, climbing, descending, turning



How ADS-B Works

Disadvantages:

- Not secured
- Easily accessible



DF: Downlink Format

CA: Capability

AA: Individual Aircraft Address

ADS-B Data: Aircraft type, Altitude, Latitude, Longitude, Airborne Velocity

PI: Parity Information (Error Detection)

ADS-B Input Mistakes

When making routine code changes, you should avoid inadvertent selection of codes 7500, 7600, or 7700 thereby causing momentary false alarms at automated ground facilities. For example when switching from code 2700 to code 7200, switch first to 2200 then 7200, NOT to 7700 and then 7200.

Important Codes

- **1200**—The VFR Code for any altitude.
- **7600**—Loss of Communications.
- **7500**—Hijacking (Never assigned by ATC with her aircraft is subject to unlawful interference).
- **7700**—Emergency (All secondary surveillance times).

Important Codes

Following is a list of important codes:

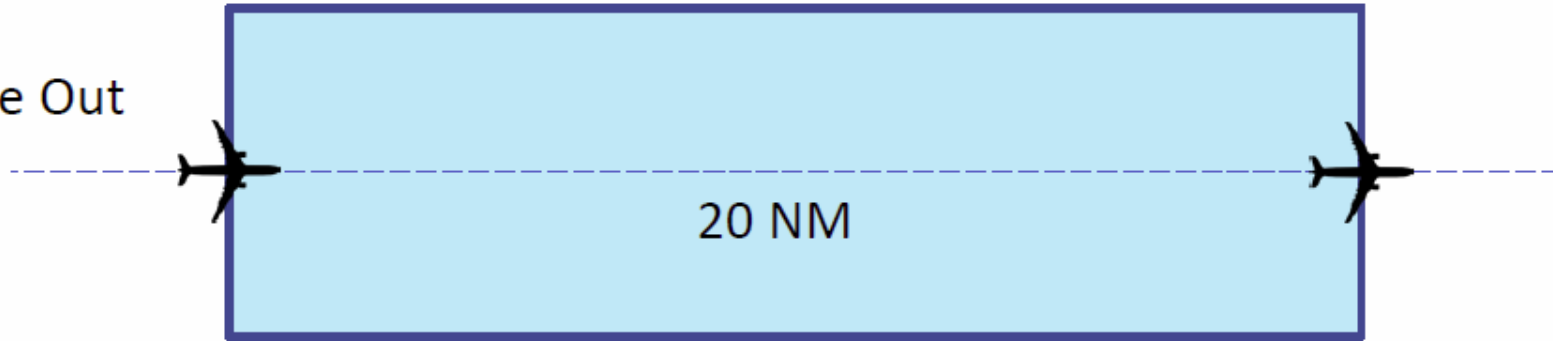
- 1200 – VFR code in the U.S. (refer to ICAO standards for VFR codes in other countries).
- 7000 – VFR code commonly used in Europe (refer to ICAO standards).
- 7500 – Hijack code.
- 7600 – Loss of communication code.
- 7700 – Emergency code.
- **7777 – Military interceptor operations code (NEVER SQUAWK THIS CODE).**
- 0000 – Code for military use in the U.S.



Decreased Separation Distance

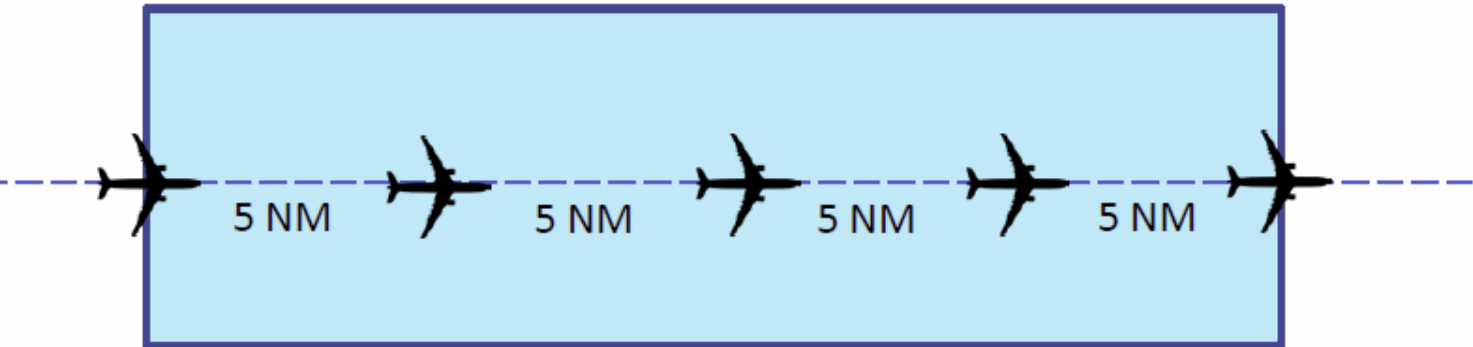
Without ADS-B Coverage

One In, One Out



With ADS-B Coverage

Separation distance decreased to 5 NM



Cyber Israel
Prime Minister's Office
National Cyber Directorate



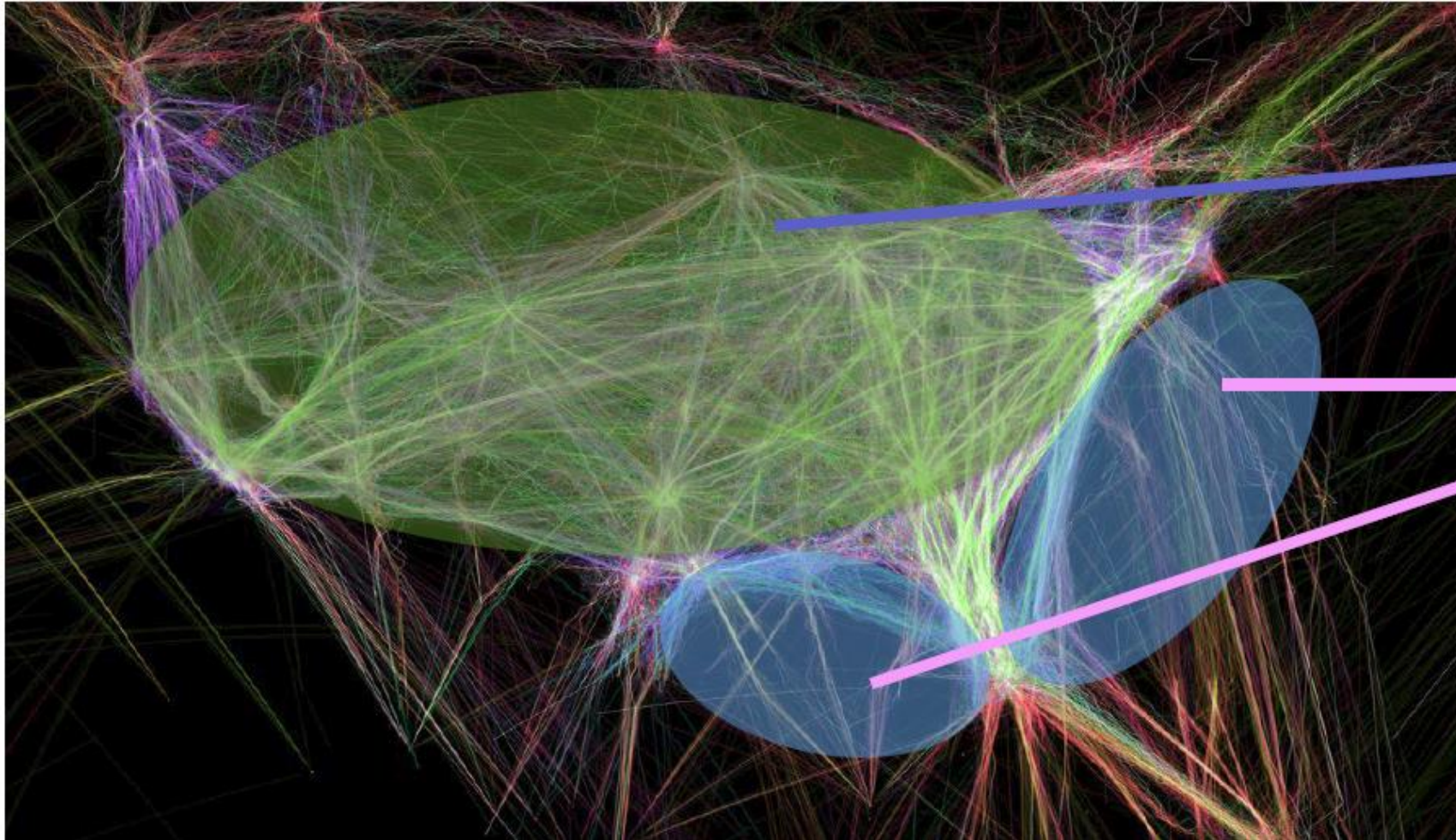
ADS-B Out VS ADS-B In

ADS-B Out is the broadcast part of ADS-B. An aircraft equipped with ADS-B Out capability will continuously transmit aircraft data such as airspeed, altitude, and location to ADS-B ground stations.

ADS-B In is the receiver part of the system. ADS-B In equipment allows aircraft, when equipped properly, to receive and interpret other participating aircraft's ADS-B Out data on a computer screen or an Electronic Flight Bag in the cockpit.



Surveillance Coverage



Radar and
ADS-B
coverage

Only
ADS-B
coverage



ADS-B Security ?

- ✈ None at all
- ✈ Attacks range from passive attacks (eavesdropping) to active attacks (message jamming, replaying, injection).
- ✈ Target selection
 - » Public Data
 - » Local data (SDR*)
 - » Virtual Aircrafts

Attacks and Affected Assets of ADS-B

THREATS	AFFECTED ASSETS		
	Confidentiality	Integrity	Availability
Attacks			
Aircraft Reconnaissance	X		
Aircraft Target Ghost Inject	X	X	X
Ground Station Target Ghost Inject		X	
Ground Station Multiple Ghost Inject		X	X
Replay Attack	X	X	
Aircraft Spoofing	X	X	
Virtual Trajectory Modification	X	X	
Aircraft Disappearance	X	X	X
False Alarm Attack	X	X	
Aircraft Flood Denial			X
Ground Station Flood Denial			X



ADS-B Threats



סייבר ישראל
Cyber Israel



Spoofing – falsification of transmitted information
False Source – creates signal that is seen as coming from an incorrect location
False Content – content within messages are altered






Flooding – floods ARTCC radar screen with ghost airplanes

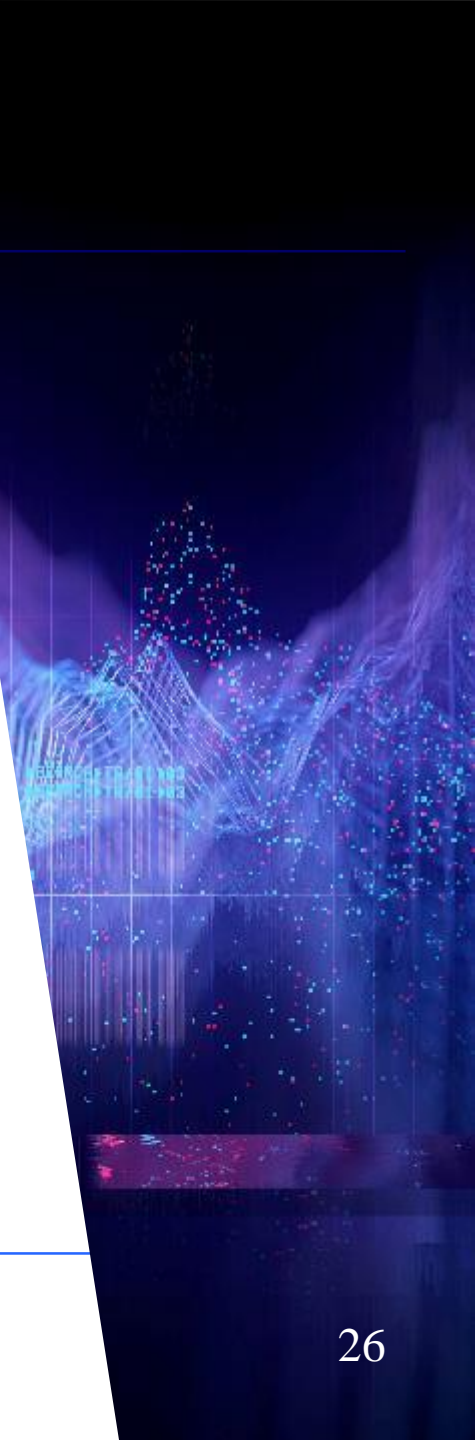
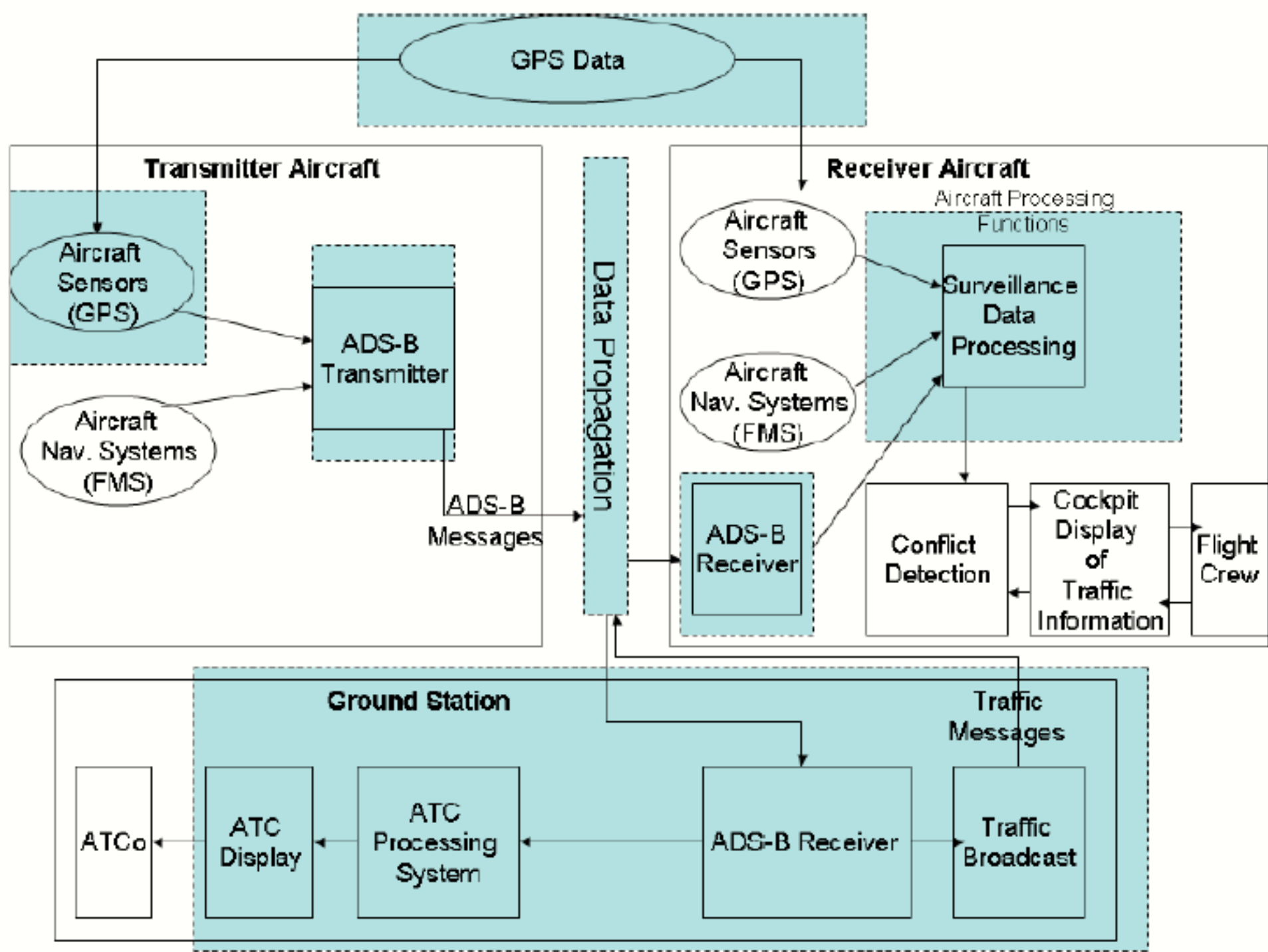
ADSB ATTACK

Truth or Fiction?

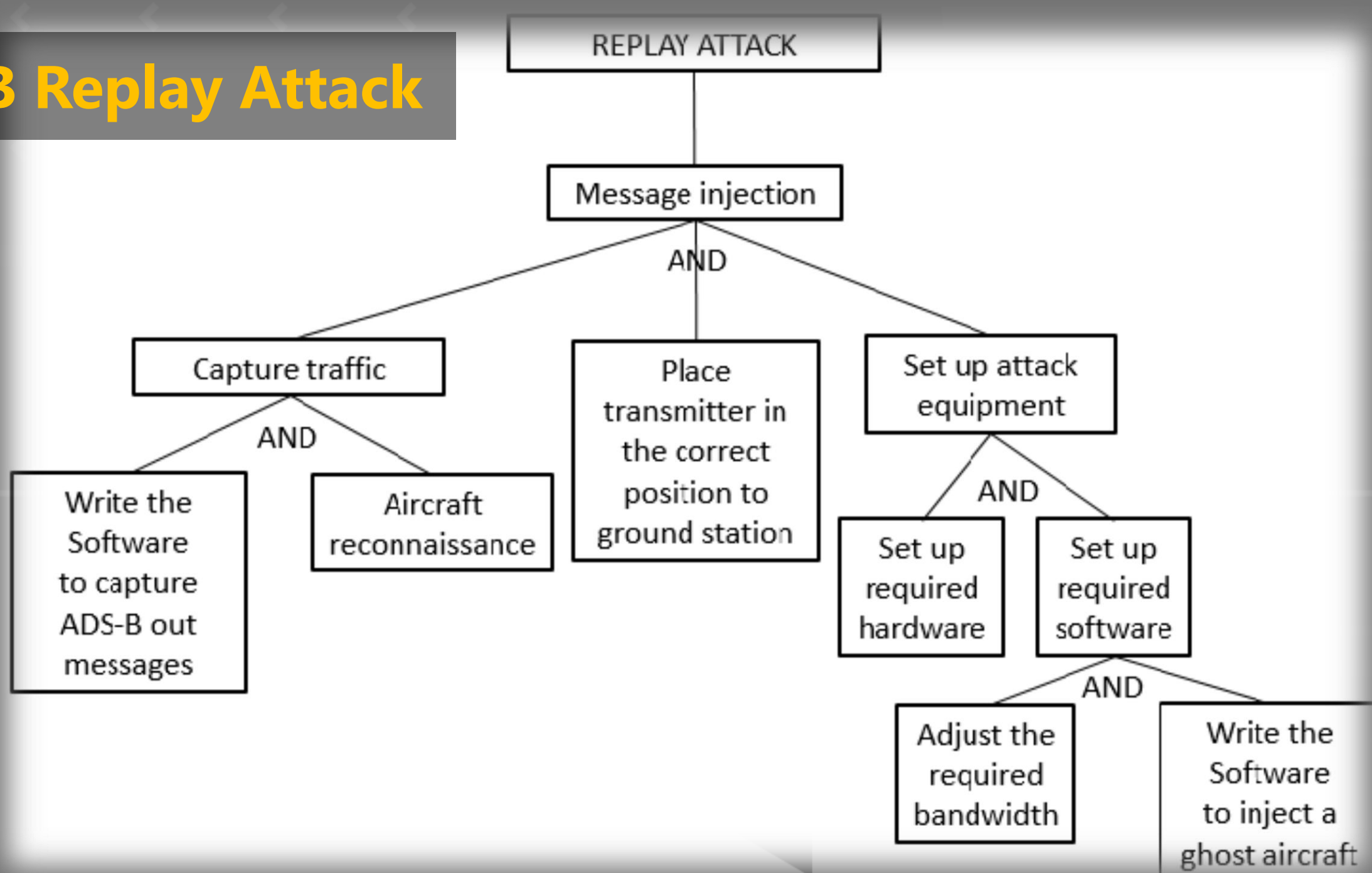


סייבר ישראל
Cyber Israel

-  **False Alarm:** In this attack an adversary deliberately injects incorrect settings into the aircraft configuration system software. This tampering can cause the aircraft configuration to appear faulty therefore leading to unauthorized flight delays. This is ranked as medium.
-  **Aircraft Target Ghost Inject:** This attack is similar to the Ground Station Target Ghost Inject, except that the goal of the adversary is to inject “phantom aircraft” into the aircraft cockpit display. This is ranked medium to high.
-  **Ground Station Multiple Ghost Inject:** By executing this attack an adversary can replace the original parameters of an ADS-B signal and insert malicious strings, designed to attack a ground station.



ADS-B Replay Attack



ADS-B Replay Attack



Target: Ground segment and air-ground segment.

Attack Technique: Message injection and interception of ADS-B OUT.

Technical Difficulty: Medium. The attacker has to perform additional steps for the message injection. The attacker must intercept and capture the data and finally to replay the captured messages making use of message injection.

Impact: 4

ADS-B Replay Attack

- Capture ADS-B data:
- UHD-mode
- *uhd_rx_cfile.py --spec B:0 --gain 25 --samp-rate 4000000 -f 1090000000 -v ~/CAPTURE_adsb.fc32*
- Pre-UHD-mode
- *usrp_rx_cfile.py*
- Replay the *captured* data:
- UHD-mode
- *tx_transmit_samples --file ~/CAPTURE_adsb.fc32 --ant "TX/RX" --rate 4000000 --freq 1090000000 --type float --subdev B:0*
- Pre-UHD-mode, *usrp_replay_file.py*

Exploitation of ADS-B Vulnerabilities



Interception of ADS-B OUT

The technique is called as aircraft reconnaissance or simply eavesdropping

Message Injection

This technique takes advantage of the ease to exploit the lack of authentication of the system



סייבר ישראל
Cyber Israel

Exploitation of ADS-B Vulnerabilities

Jamming

The execution of jamming disables one of various nodes in the wireless network from sending or receiving messages with enough power to disrupt 1090MHz frequency

Message Deletion

This attack is executed mainly by means of interference to delete messages from the wireless network



Exploitation of ADS-B Vulnerabilities



Message Modification

The integrity of the message is affected with the modification of the information contained in the message. The technique might be performed by two means, overshadowing and bit-flipping



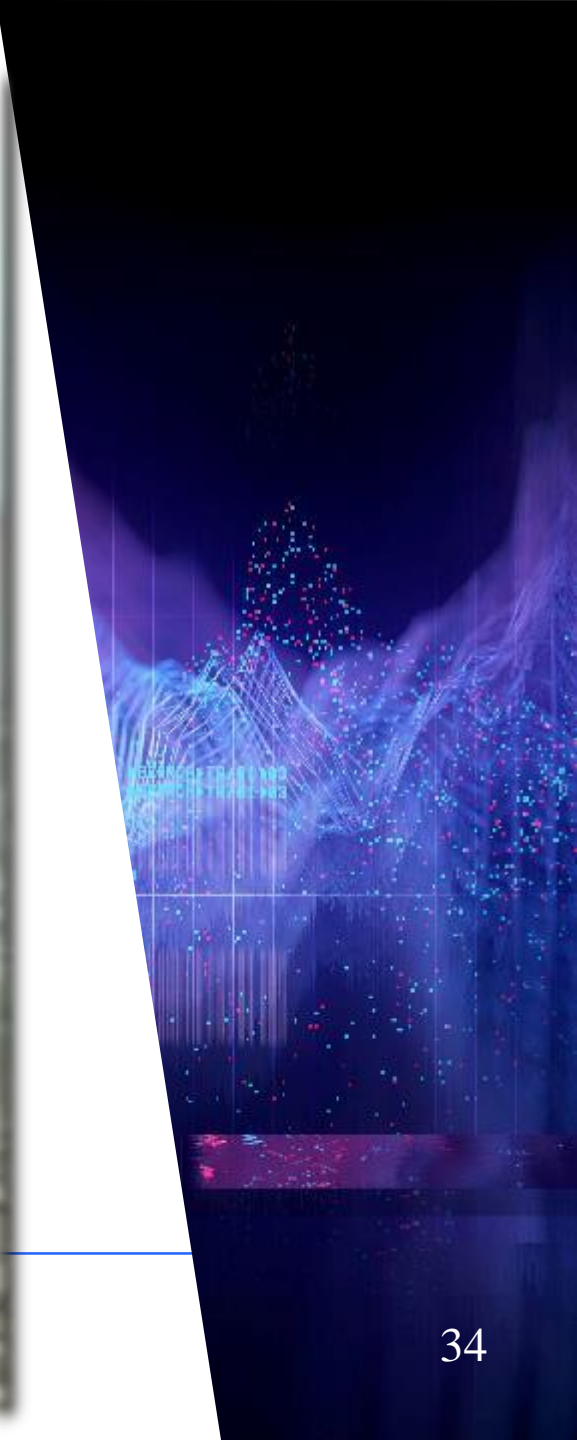
סייבר ישראל
Cyber Israel

ADS-B ?



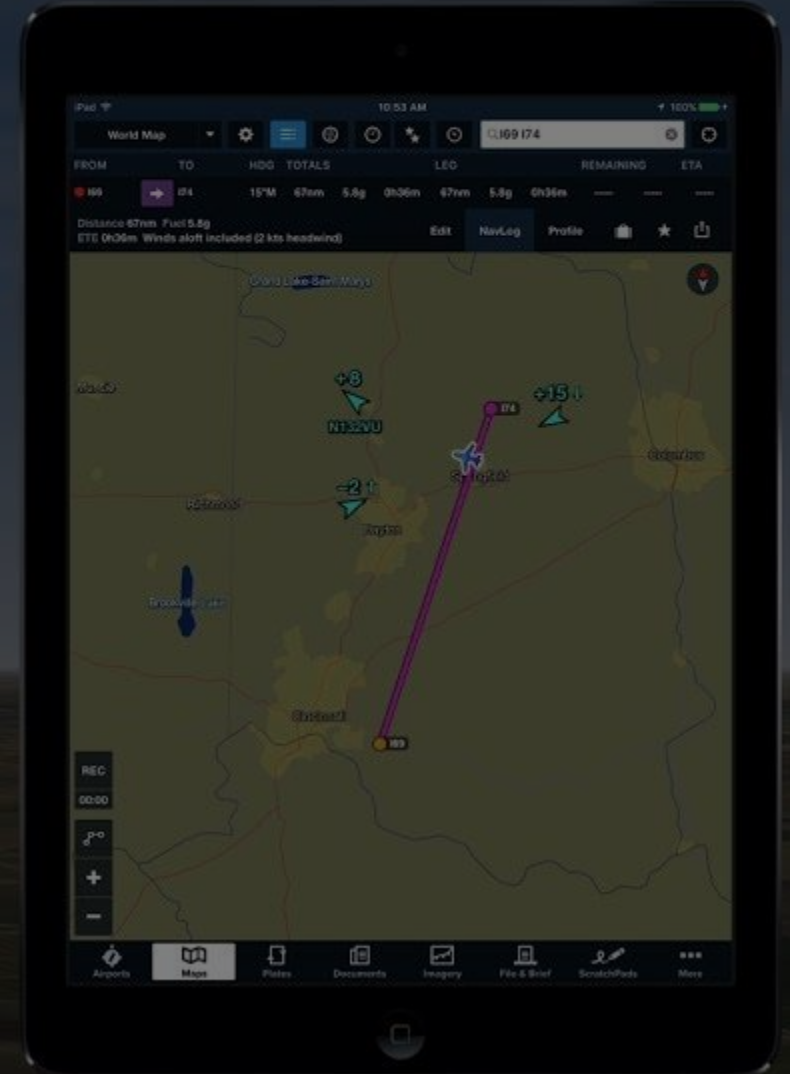
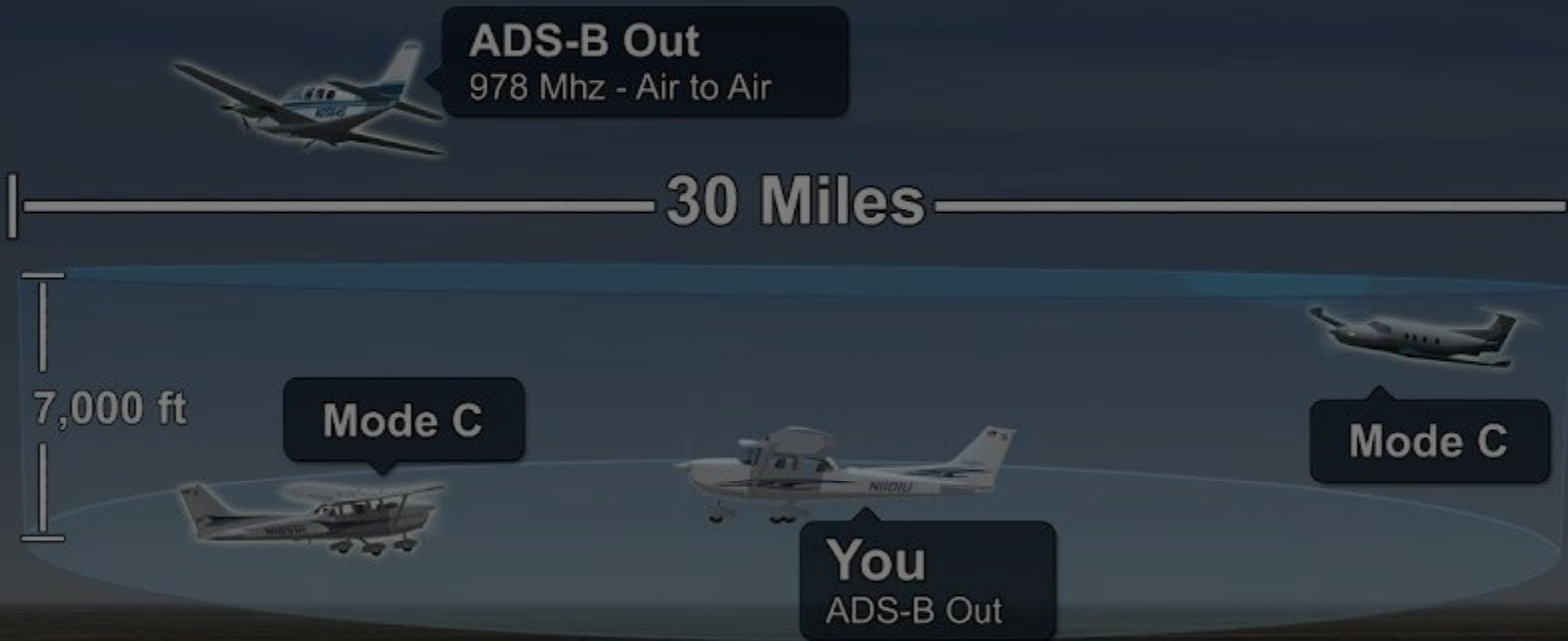


What can happen when ADS-B sabotaged



How does ADS-B look like ?

Community view



Summary

ENCOURAGE AVIATION TO WORK TOGETHER ON THE DISCOVERY,
RESEARCH AND MITIGATION OF CYBER THREATS

ADS-B require **real security in-place** in order to operate safely and
according to the requirements

BUILDING INFORMATION AND ASSISTANCE **SHARING CHANNELS (CERT)**

Thank You!



סייבר ישראל
Cyber Israel

מערך הסייבר הלאומי - משרד ראש הממשלה
National Cyber Directorate - Prime Minister Office

Tom Alexandrovich

Aviation Guidance Manager
Critical Infrastructures Division

TomA@cyber.gov.il