# Critical Infrastructure Security

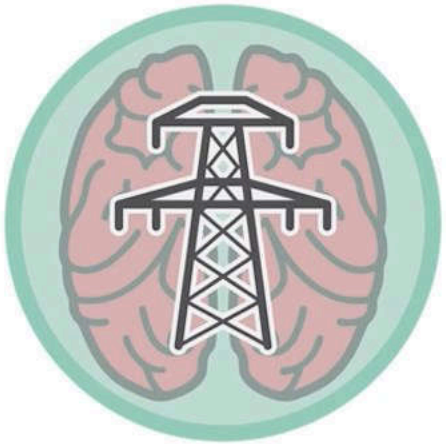
## Lecture 7

Dr. Naveed Anwar Bhatti

**Webpage:** naveedanwarbhatti.github.io

# SECURING SMART GRID

# Securing Smart Grid



The consequences of a cyber attack against the Smart Grid range from espionage to sabotage, and from petty theft to larger privacy concerns

# Securing Smart Grid

The consequences of a cyber attack against the Smart Grid range from espionage to sabotage, and from petty theft to larger privacy concerns

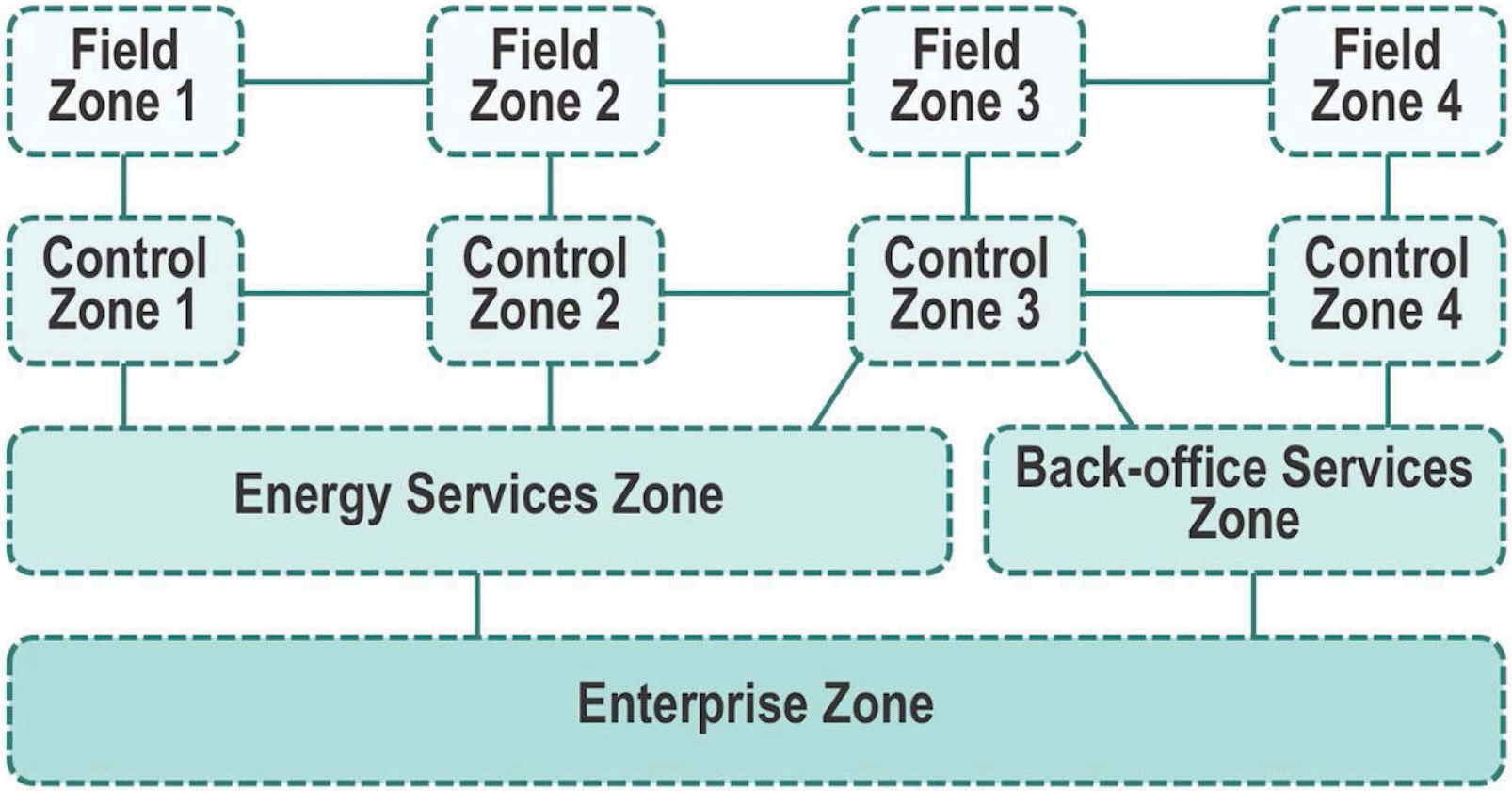
While no one product or technology is certain to stop all attacks, when used together in a defense-in-depth posture across all areas of the Smart Grid, it is possible to greatly minimize the risk of a successful cyber attack.

# Securing Smart Grid

It is therefore necessary to—above all else—establish appropriate monitoring of all Smart Grid systems to obtain situational awareness.

By looking at the entirety of a system's digital behaviors, areas of risk can be identified, attacks can be detected, and suspicious or dangerous trends can be identified.

# Securing Smart Grid

# FIELD ZONE PROTECTION

Field devices are often embedded systems.

Low cost and low power consumption

Smart grid owner is unable to alter these devices, or install any commercially available cyber security countermeasure.

# FIELD ZONE PROTECTION

Field devices are often embedded systems.

Low cost and low power consumption

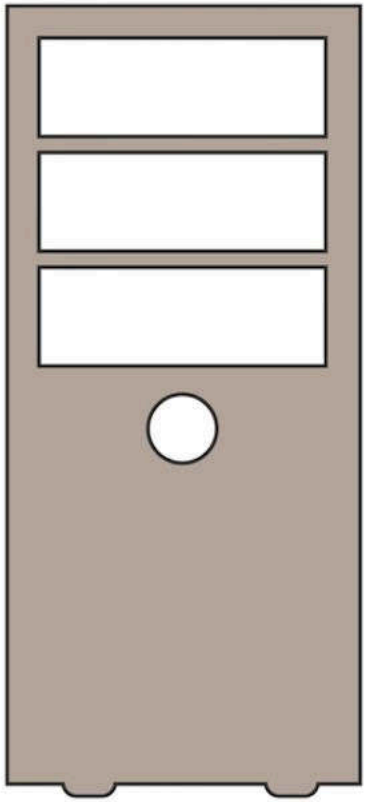
Smart grid owner is unable to alter these devices, or install any commercially available cyber security countermeasure.

Onus falls to the device manufacturer to build cyber security.

Application whitelisting is one of the more popular software security solutions for embedded devices.

Activate Windows

# CONTROL ZONE PROTECTION



As we move further in from the field and into the substations, we see more sophisticated devices (e.g., SCADA servers, measurement and data management servers, AMI headends, and similar server-based systems).

# CONTROL ZONE PROTECTION

## Technologies deployed:

- Application whitelisting
- Antivirus
- Configuration management

# CONTROL ZONE PROTECTION

Technologies deployed:

- Full system hardening
- Separation of services (either to dedicated hardware or to individual virtual machines if virtual data centers are utilized)
- Host IDS or Host IPS
- Host data loss prevention (DLP)
- Event logging

Activate Windows

# SERVICE ZONE PROTECTION AND BACK-OFFICE SYSTEMS

As we get to centralized SCADA systems, historians, data concentrators, and back-office systems, the capabilities of the servers increase, as does the value of the data.

There is an increased reliance upon the integrity of data and less on availability since we are moving away from real-time control to more transaction-based information.

Data integrity and information assurance tools, including database security solutions, database auditing, and data loss prevention tools in these areas.

Activate Windows
Go to Settings to activate Windows.

# Advance Network Monitoring

SIEM or Log Management Tool

NETWORK FORENSICS

# Drones and Critical Infrastructure

Understanding the DRONE Threat Space

# Drones and Cyber Security

## Drone as target

Critical law enforcement or data collection missions using drones could be undermined by cyberattacks on these platforms

## Drone as Vector

Drones in the hands of adversaries could present novel avenues for cyberattacks, with drones themselves serving as “cyber weapons” intended to deliver malicious content or kinetic impacts

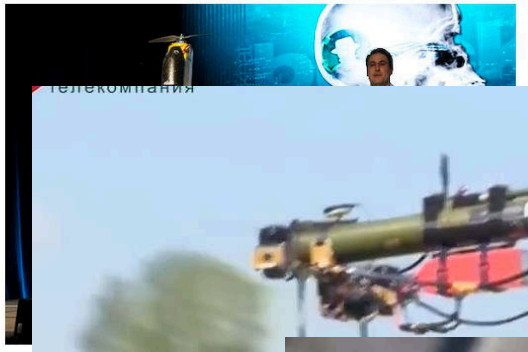
# Drone as Vector

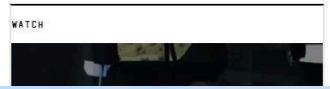
## Drones as a threat

- Flying computers. *(I*
- Custom payloads:
  - Sniffers
  - Jammers
  - Network Analyzers
  - 3d mapping, cameras.
  - Physical attacks, explosives.
  - …

**DIY Spy Drone Sniffs Wi-Fi, Intercepts Phone Calls**

What do you do when the target you're spying on slips behind his home security gates and beyond your reach? Launch your personal, specially-equipped drone to fly overhead and sniff his Wi-Fi network, intercept his cellphone calls, or launch denial-of-service attacks with jamming signals.








# Our Focus

## Drone as target

Critical law enforcement or data collection missions using UAS could be undermined by cyberattacks on these platforms

## Drone as Vector

UAS in the hands of adversaries could present novel avenues for cyberattacks, with UAS themselves serving as “cyber weapons” intended to deliver malicious content or kinetic impacts

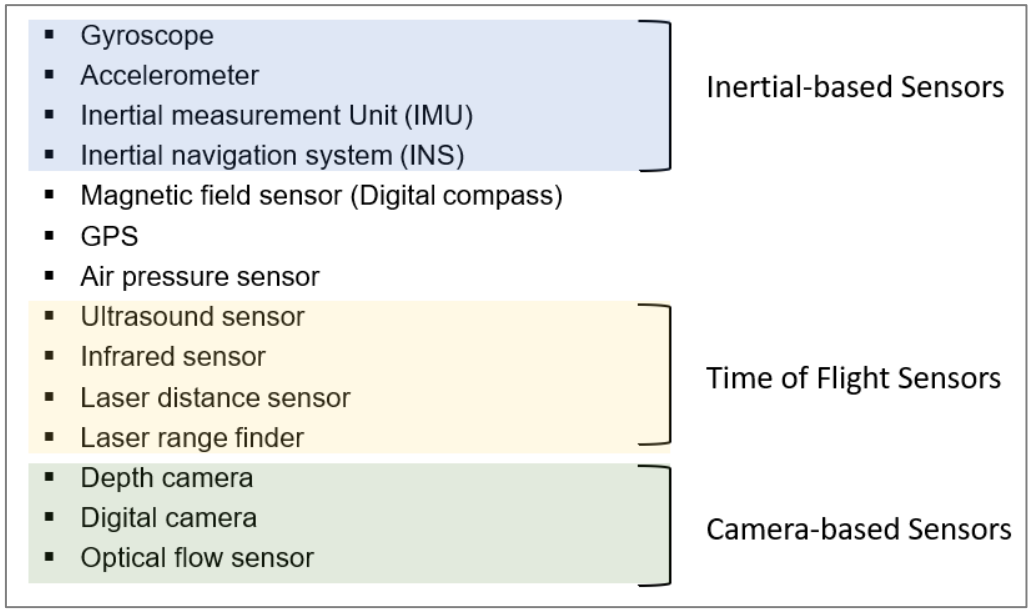
**Threat** | **Vulnerability** | **Attack**

# Drone-Related Attack Surfaces

- Sensors
- Navigation
- Air Traffic Control
- Fault Handling
- Application Layer
- Physical Layer
- Link Layer
- Network Layer
- AI

# Sensors (+ Navigational Sensors)

- Drones are data-driven systems
  - Sensors: Eyes and Ears of the pilot
- Example of Sensors




- Spoofing/Tempering: Exploiting the limitation of sensors
  - Manipulation of visual inputs
  - Manipulation of EM in sensors
  - Manipulation of auditory/physical inputs
- Jamming:
  - Saturation of sensory limits (e.g. laser light on Camera CCDs)
  - EM disruption

# GPS Jamming and Spoofing

- Global Navigation Satellite System (GNSS)
  - constellation of satellites transmit position and timing data to receivers

Jamming

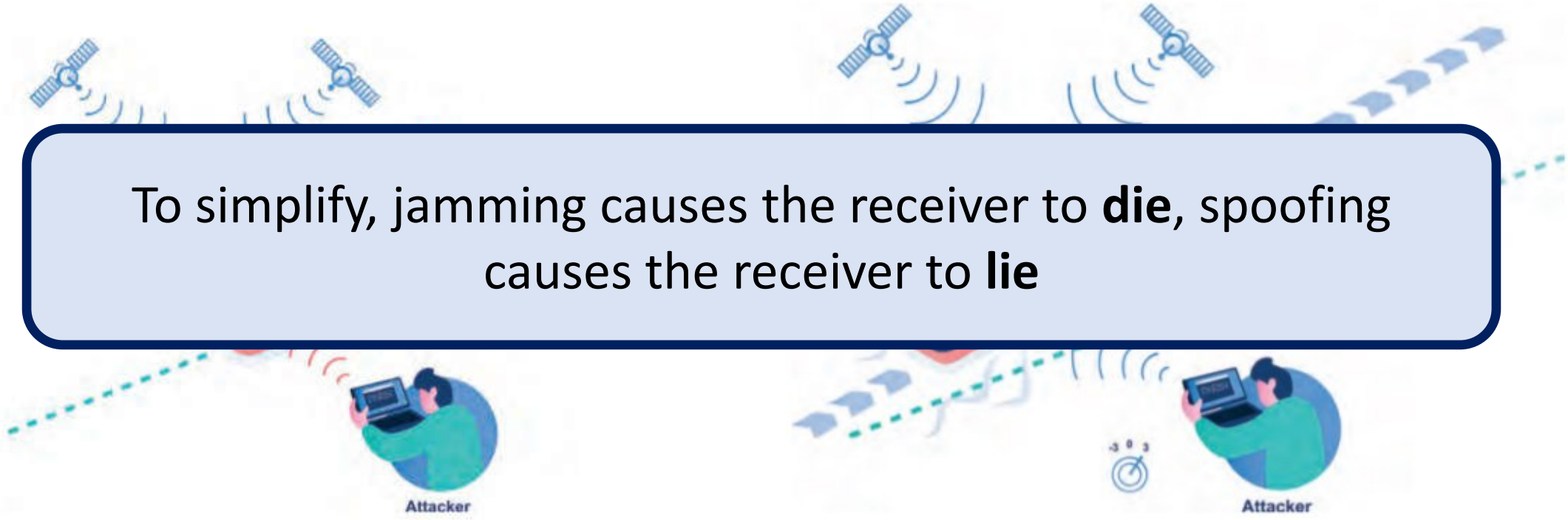

Spoofing/Tempering

# GPS Jamming and Spoofing

- Global Navigation Satellite System (GNSS)
  - constellation of satellites transmit position and timing data to receivers

Jamming

Spoofing/Tempering




To simplify, jamming causes the receiver to **die**, spoofing causes the receiver to **lie**

# GPS Jamming and Spoofing

- Global Navigation Satellite System (GNSS)
  - constellation of satellites transmit position and timing data to receivers

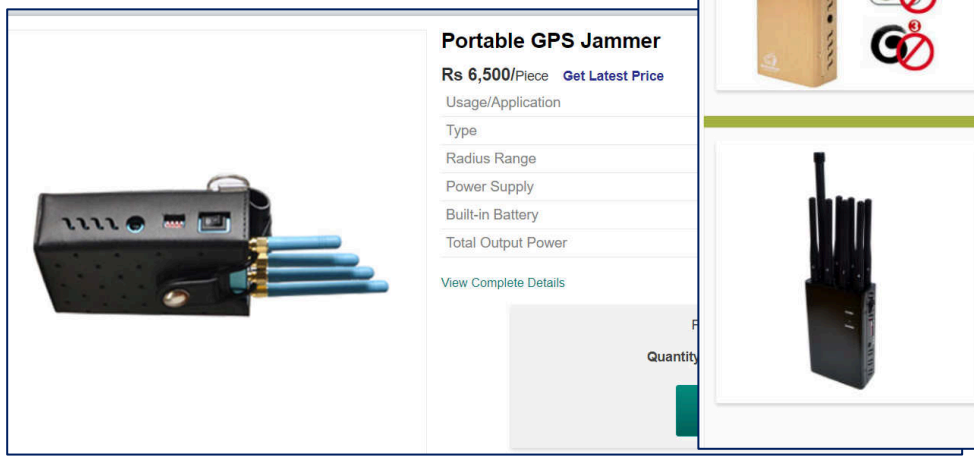
- Jamming
  - GNSS signals have low power
  - Jammed by masking the satellite signal with noise on GNSS Frequencies
  - Readily available and inexpensive

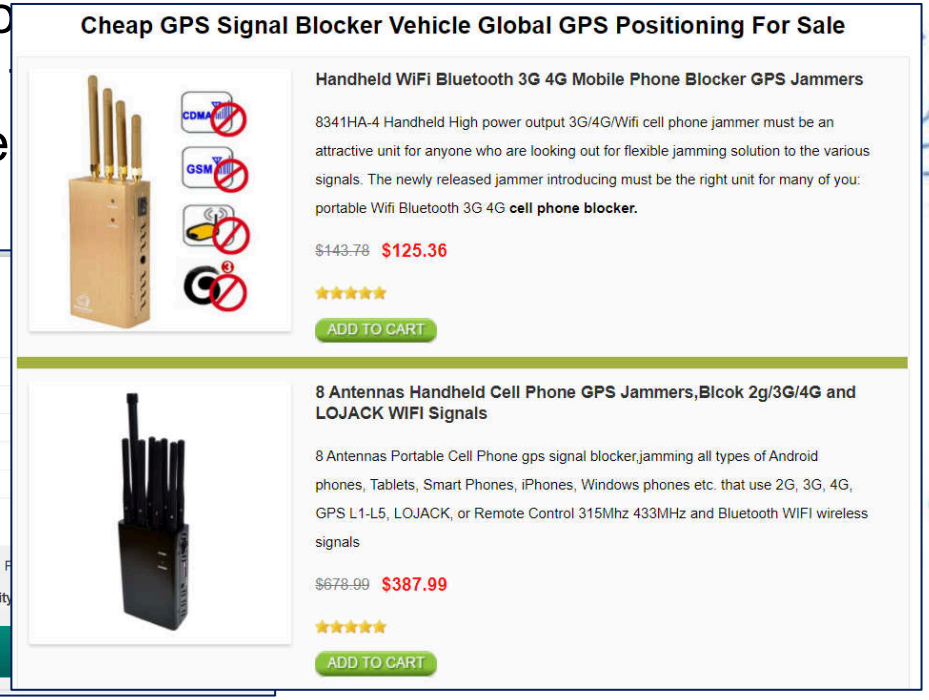
Jamming

# GPS Jamming and Spoofing

- Global Navigation Satellite System (GNSS)
  - constellation of satellites transmit position and timing data to receivers

- Jamming
  - GNSS signals have lo
  - Jammed by masking
    on GNSS Frequencie
  - Readily available and




Jamming

# GPS Jamming and Spoofing

- Global Navigation Satellite System (GNSS)
  - constellation of satellites transmit position and timing data to receivers

- Spoofing
  - Provision of GNSS-like signals, transmitted locally and coded to fool the receiver to think it is somewhere it is not.

  - Begins by broadcasting signals synchronised with the genuine signals. The power of the counterfeit signals is then gradually increased so that the victim's GNSS receiver tracks the false signals which can then be manipulated to report a different location to the genuine signals

Spoofing

# GPS Jamming and Spoofing

- Global Navigation Satellite System (GNSS)
  - constellation of satellites transmit position and timing data to receivers

- Meaconing
  - Type of spoofing where GNSS signals are re-transmitted
  - Requires simpler equipment than that required for a spoofing attack

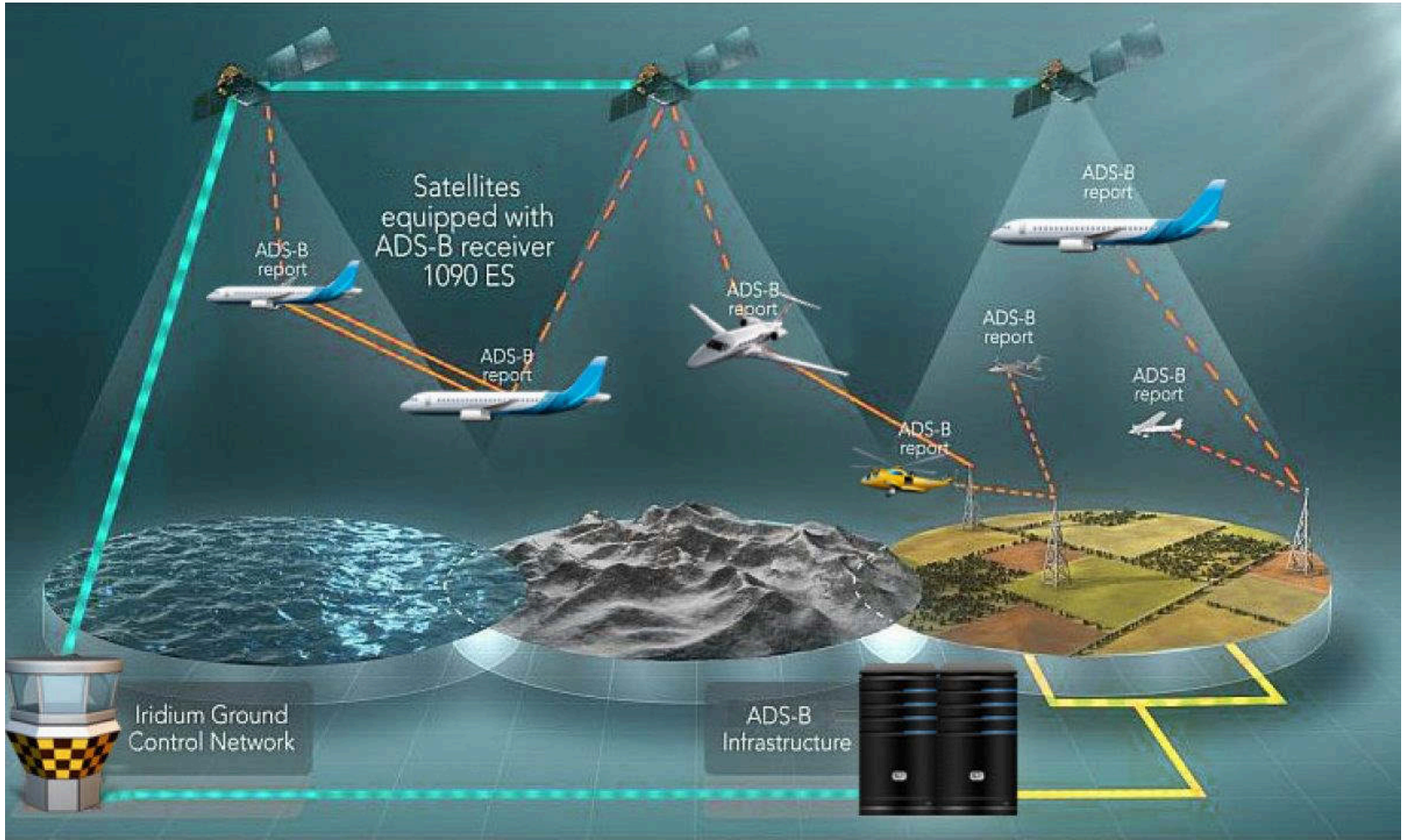
Spoofing

# GPS Jamming and Spoofing

- Global Navigation Satellite System (GNSS)
  - constellation of satellites transmit position and timin
- Meaconing
  - Type of spoofing where GNSS signals are re-transmitted
  - Requires simpler equipment than that required for a spoofing attack

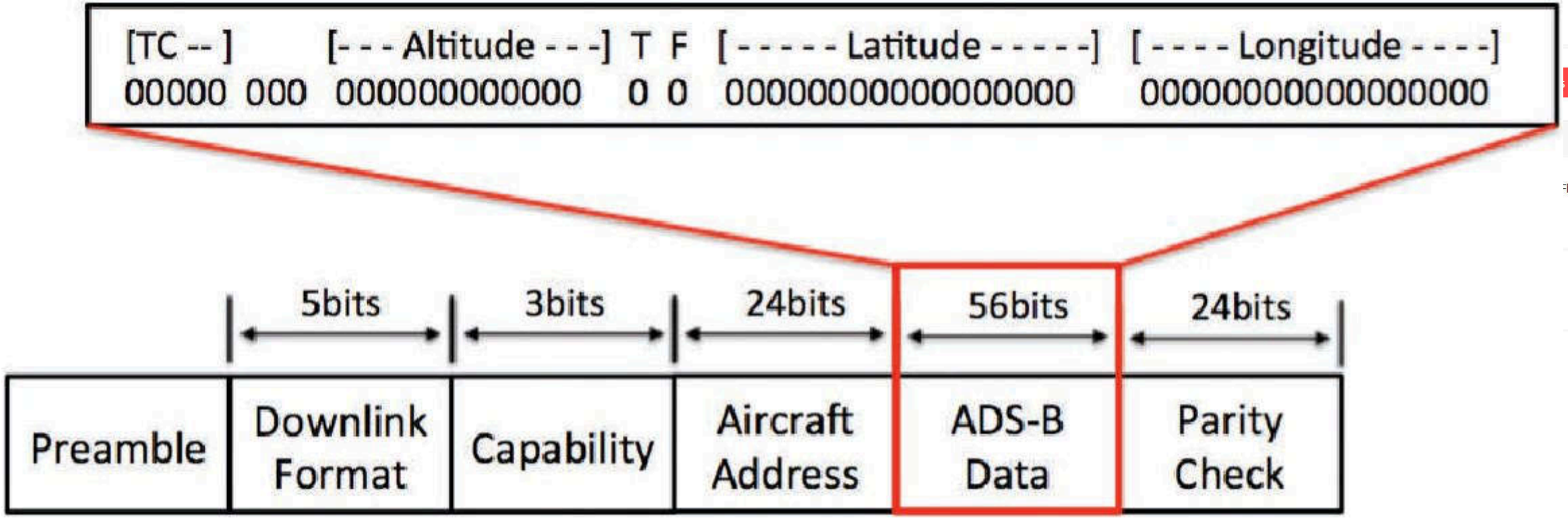
# Air Traffic Control

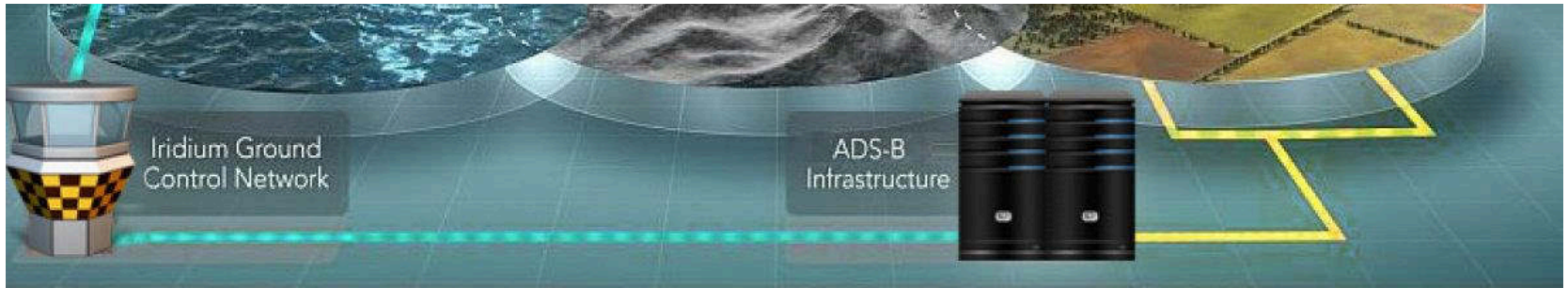
- Traffic Monitoring and Collision Avoidance tools
  - ADS-B and TCAS



# Air Traffic Control

- Traffic Monitoring and Collision Avoidance tools



# Air Traffic Control

- Traffic Monitoring and Collision Avoidance tools
  - ADS-B and TCAS

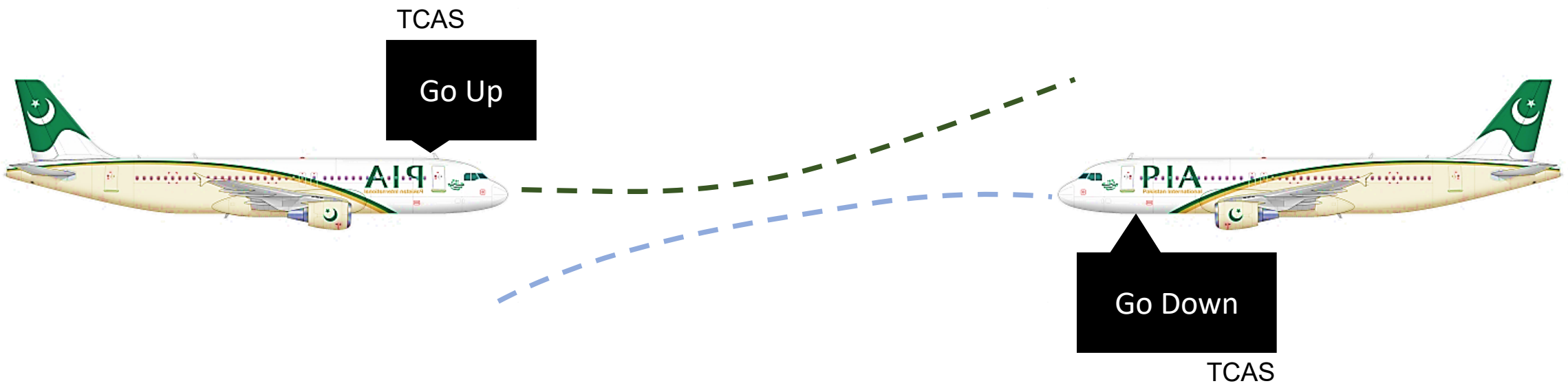
# Air Traffic Control

- Traffic Monitoring and Collision Avoidance tools
  - ADS-B and TCAS

# Air Traffic Control

- Traffic Monitoring and Collision Avoidance tools
  - ADS-B and TCAS

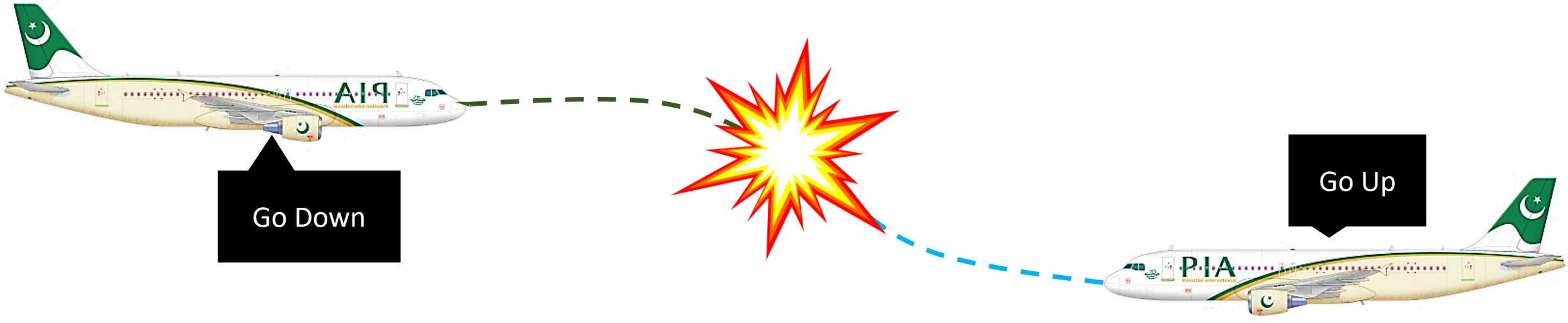
- Collision induction through collision avoidance



# Air Traffic Control

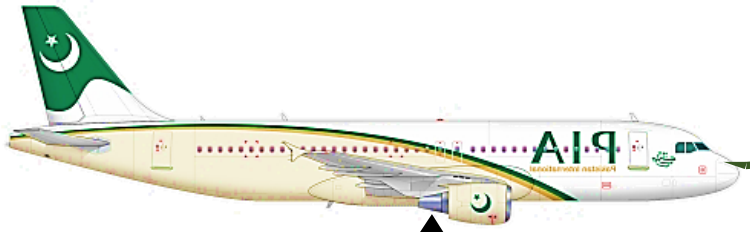
- Traffic Monitoring and Collision Avoidance tools
  - ADS-B and TCAS

- Collision induction through collision avoidance

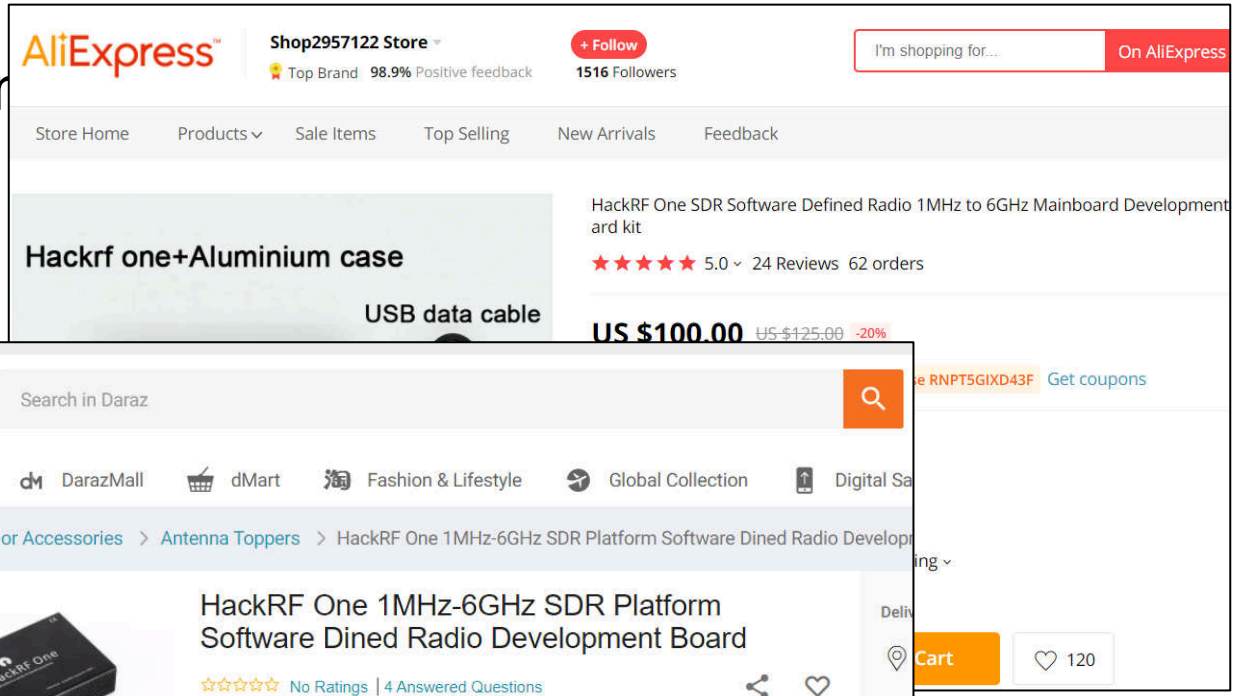


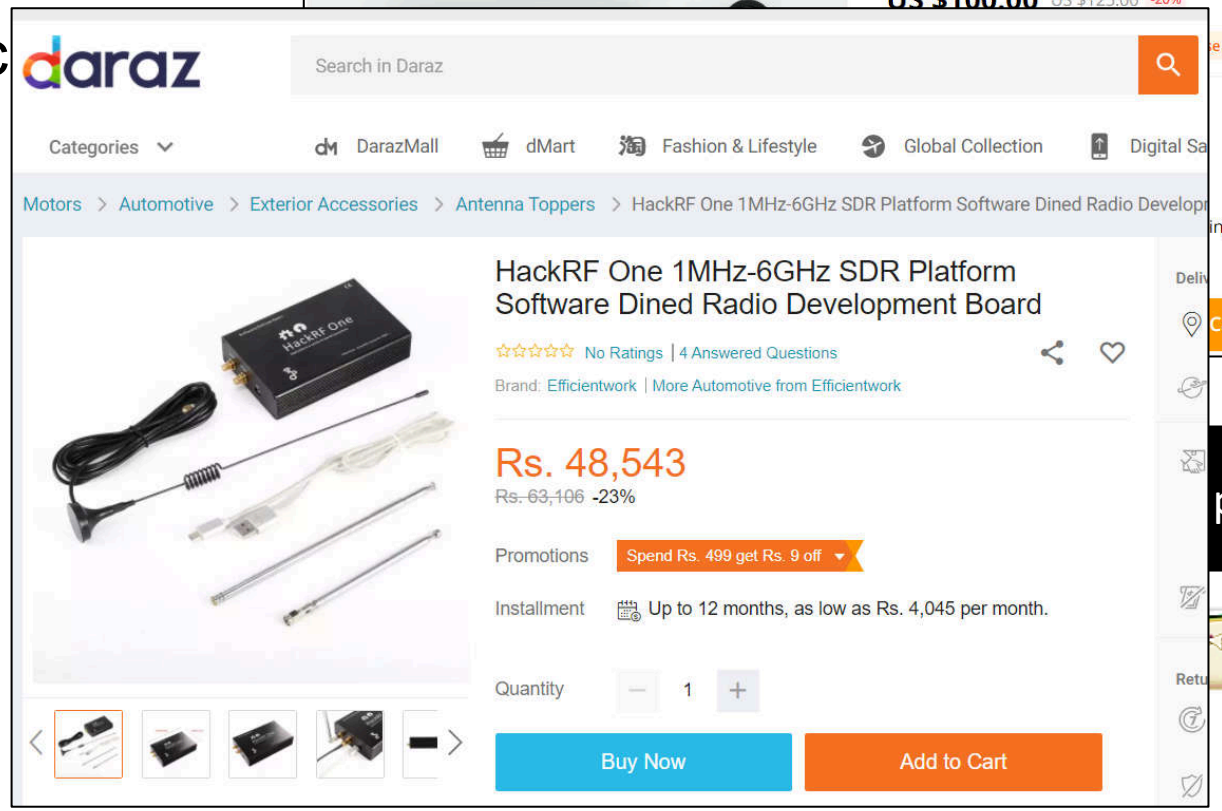
# Air Traffic Control

- Traffic Monitoring and Collision Avoidar
  - ADS-B and TCAS
- Collision induction through c




Go Down



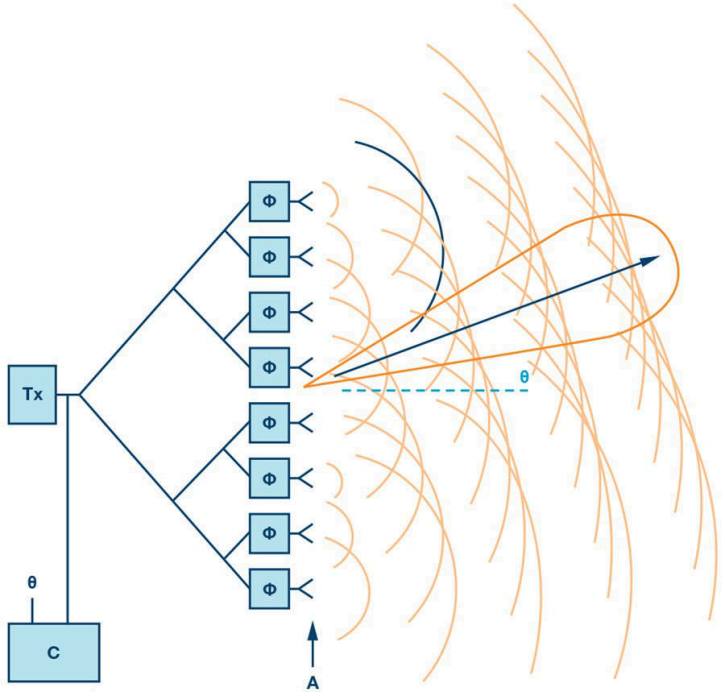




# Fault Handling

- Induction of fail-safe mechanism
  - Hover **(make kinetic attacks and capture easier)**
  - Return to base **(combined with navigation attacks may lead to capture)**
  - Land **(=capture)**
  - Self-destruct

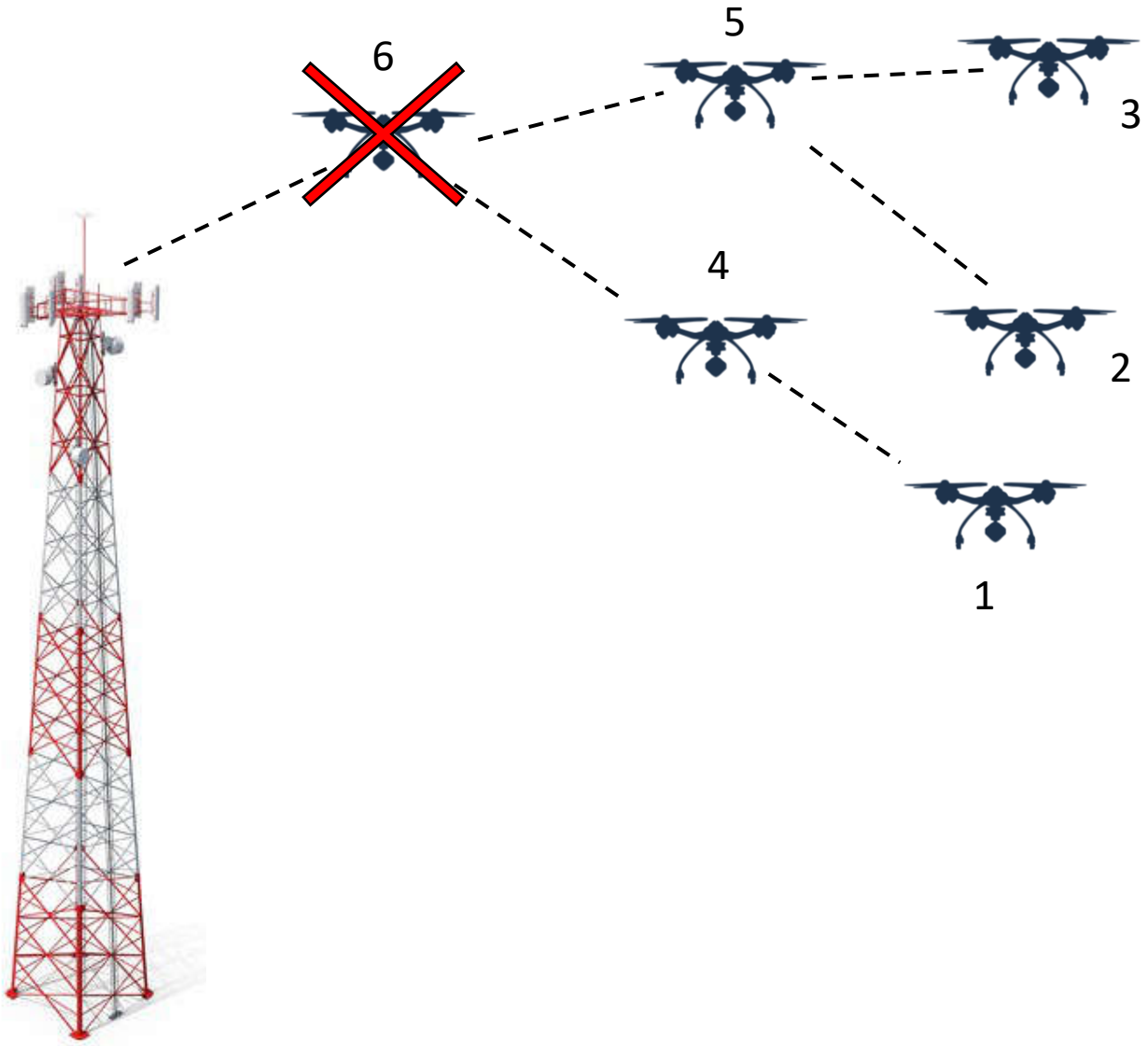
# Physical Attack

- **Adaptive Radios**: Manipulation of environmental parameters (spectrum sensing)
- Manipulation of anti-jamming solutions such as direction of arrival estimation in **Beamnulling**
- Exploiting of antenna pattern and orientation (TCAS Attack)



# Link Layer and Network Layer

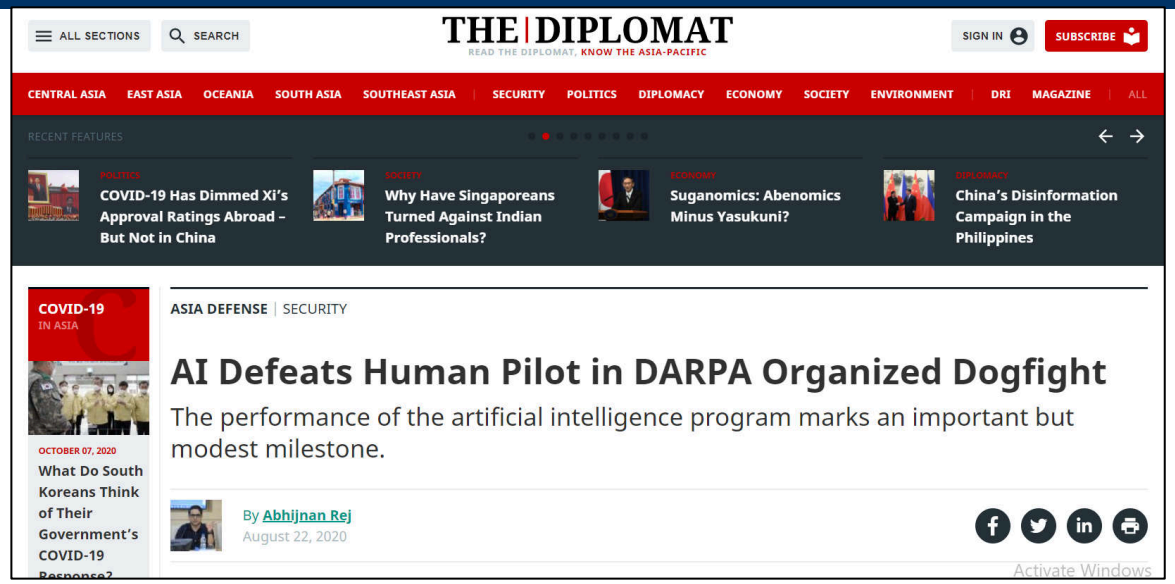
- Traffic Analysis
- Topological Attacks on multi-UAV
- Routing Attacks (Black Holes)

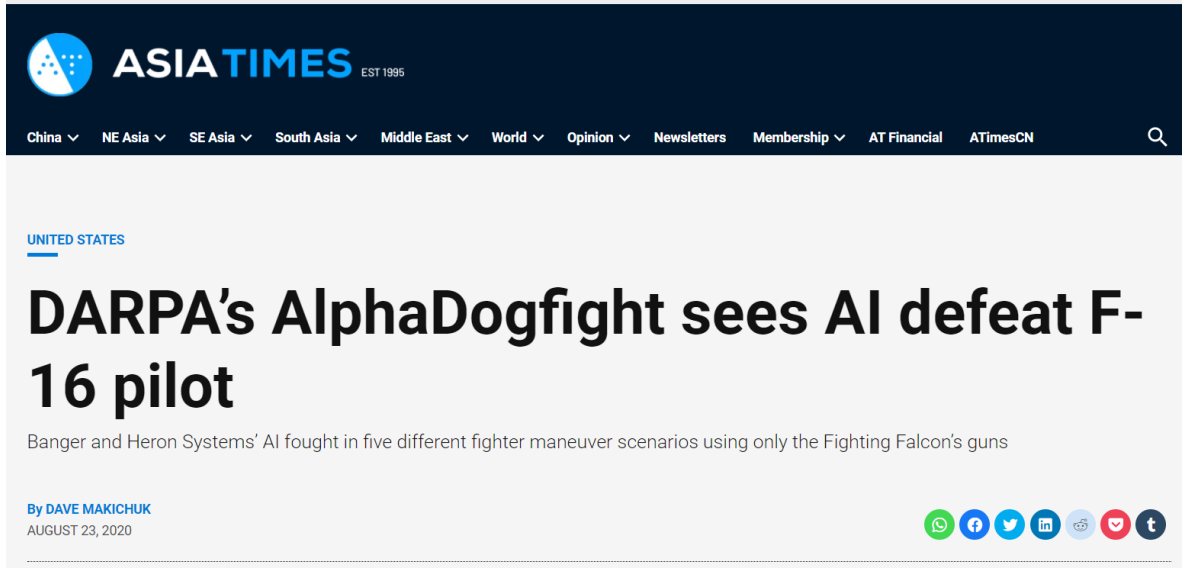


# Artificial Intelligence

**Them: "AI is going to take over the world and kill us"**

**Meanwhile AI:**

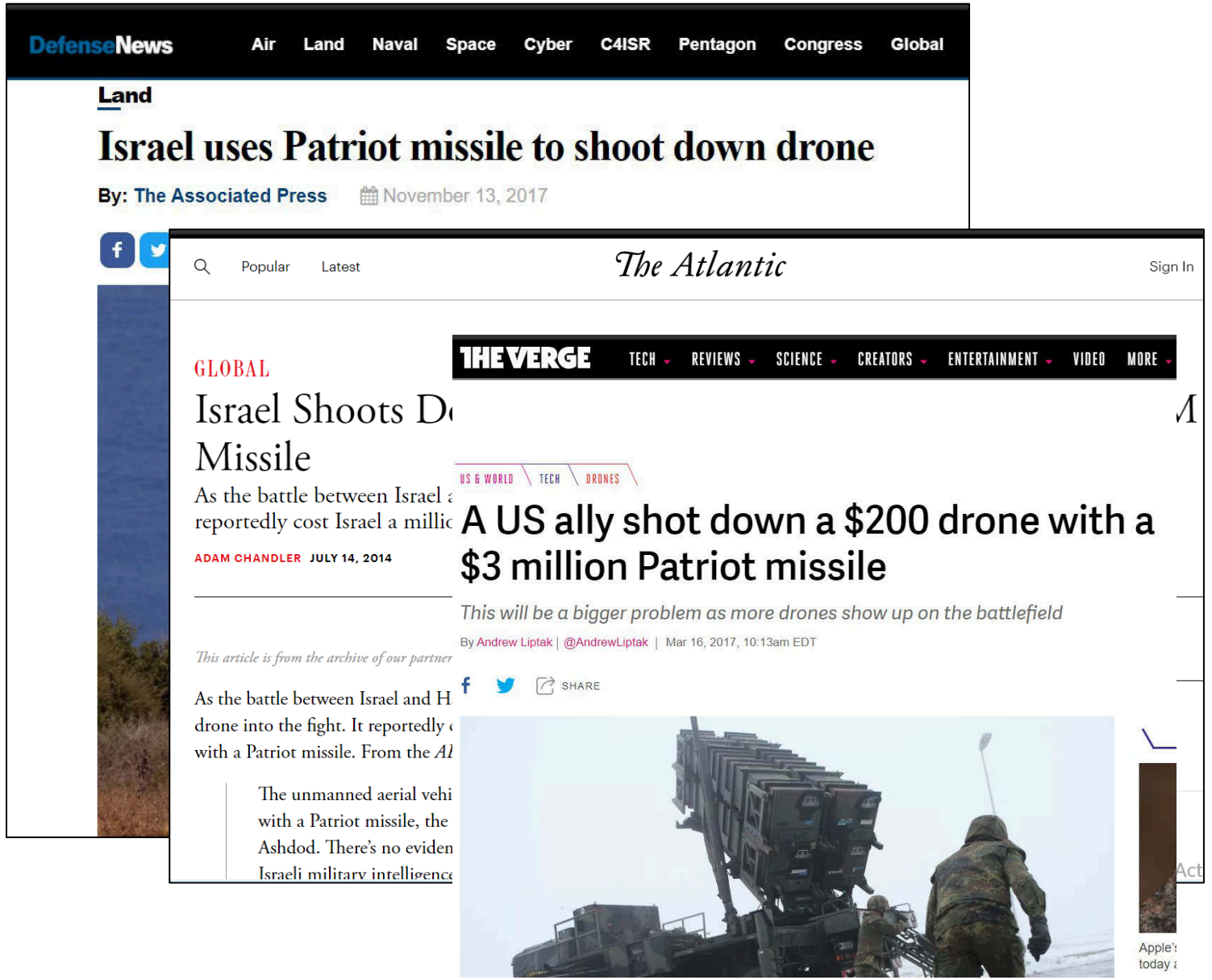



Can we use the exploits in meaningful way?

## ANTI-DRONE technology

# Solutions

## Israel Way



# Solutions

American Way

JORDAN GOLSON 08.27.15 07:00 AM

## Welcome to the World, Drone-Killing Laser Cannon


3 Billion Dollars

# Solutions

## French Way

Sections

The Washington Post
*Democracy Dies in Darkness*

Get 1 year for $29

WorldViews

**Terrorists are building drones. France is destroying them with eagles.**


Like 16.5M

Monday, Oct

**Mail Online**

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money

Latest Headlines | Coronavirus | Royal Family | Crime | Boris Johnson | Prince Harry | Meghan Markle | World

**Eagle trained to bring down terrorist drones attacks a five-year-old girl enjoying a picnic after it mistook her white T-shirt for an enemy**

- Eagle trained to swat drones out of the sky mistook a girl for one of the devices
- Youngster, five, was enjoying a picnic when the huge bird swooped down on her
- It left her with 'minor injuries' and air force personnel apologised to the group
- Eagles are trained to claw drones that could be used by terrorist to carry bombs

By PETER ALLEN IN FRANCE FOR MAILONLINE
**PUBLISHED:** 17:24 BST, 7 June 2018 | **UPDATED:** 21:36 BST, 7 June 2018

Share 173 shares 107 View comments

A French airforce eagle designed to claw drones out of the sky attacked a five-year-old girl dressed in white because she looked like one of the aircraft.

The drama took place in the picturesque Col d'Aubisque – a mountain pass in the Pyrenees close to the South West town of Tarbes.

English

euronews.

Search Newsletters

Europe World Business Sport Culture Living Sci-tech Travel Video Programmes Live

BREAKING NEWS • Paul R Milgrom and Robert B Wilson win the 2020 Nobel Prize in Economics for improvements to auction theory and inventions of new auction formats

Home > News > World > Where Eagles Dare: France trains birds to bring down drones

FRANCE

**Where Eagles Dare: France trains birds to bring down drones** COMMENTS

By Catherine Hardy • last updated: 16/02/2017

SHARE THIS ARTICLE

TEXT SIZE Aa Aa

# Solutions

Pakistani Way

Bullets < 1$

# Thanks a lot

If you are taking a Nap, **wake up**.....Lecture Over